1

unlimited

Convex Models of Malfunction Diagnosis In High Performance Aircraft

Yakov Ben-Haim
Department of Nuclear Engineering
Technion — Israel Instit~~ute~~ of Techn~~ology~~
Haifa, ~~Israel~~ 32000

Final Report
May 1989

Funded by the Air Force Office of Scientific Research
Grant Number AFOSR-88-0209

Convex Models of Malfunction Diagnosis In High Performance Aircraft

Yakov Ben-Haim
Department of Nuclear Engineering
Technion — Israel Institute of Technology
Haifa, Israel 32000

Final Report
May 1989

Funded by the Air Force Office of Scientific Research
Grant Number AFOSR 88 0209

Contents

STATEMENT "A" per D. Tyrell
AFOSR/XOTD(~~TIC~~)
TELECON 2/16/90 CG

1 Statement of the Problem

This project is devoted to the study of diagnosis of additive malfunctions in linear dynamic systems. This class of failures is relevant to control-actuator failures in aircraft, as well as to other situations. In particular, we are interested in optimizing multi-hypothesis maximum-likelihood algorithms for malfunction diagnosis, since this concept is the most widely accepted basis for automatic malfunction diagnosis.

The engineering system to be studied is a linearized aerodynamic model for small disturbances about a reference condition of steady rectilinear flight over a flat earth. The advantage of this system is its simple description of a wide range of aerodynamic situations, and the fact that control-actuator malfunctions can be modelled as additive failures.

The formulation of a multi-hypothesis algorithm for malfunction diagnosis involves the choice of a set of hypothesized malfunctions. On-line measurements of the system are compared with the behavior to be expected from each hypothesized failure, and a likelihood-ratio algorithm is used to identify the hypothesized failure which is most likely to have given rise to the observed measurements. Optimization of such an algorithm centers on the choice of the set of failure hypotheses: How many failure hypotheses should be chosen, and what should those failure hypotheses be?

The methodology of convex modelling presented in this report is to be used to address these questions. Convex modelling provides two distinct tools for optimization of malfunction diagnosis algorithms. The first, called ***benchmark diagnosis***, is an assessment of the best state space malfunction diagnosis capability which can be obtained by any state space algorithm, whether based on the multi-hypothesis maximum-likelihood concept or not. Evaluation of the optimum diagnosis capability is used as a benchmark, against which the performance of implementable algorithms can be compared. The second tool provided by convex modelling, called ***multi-hypothesis distinguishability***, enables assessment of the malfunction diagnosis performance of a specific multi-hypothesis algorithm. This enables the quantitative comparison of the performance of multi-hypothesis malfunction diagnosis algorithms based on distinct sets of failure hypotheses. Optimization of the malfunction diagnosis algorithm is based on these comparisons. For example, the performance of different sets containing N failure hypotheses can be compared, and the best set of hypotheses can be sought. Furthermore, the utility of the marginal $((N + 1)$th) hypothesis can be established by comparing the best N-fold set of hypotheses with the best $(N + 1)$-fold set. Finally, the multi-hypothesis diagnosis capability of any specific implementable algorithm can be compared with the best possible malfunction diagnosis capability, as expressed by the benchmark distinguishability. In this way, rational design decisions can be made in the formulation of a multi-hypothesis maximum-likelihood algorithm for malfunction diagnosis.

2 Background and Approach

The diagnosis of additive malfunctions in linear dynamic systems has been studied from various points of view. Fiorina and Maffezzoni (1979) use the generalized likelihood ratio to detect additive step failures in the Italian power system. Kerr (1982) discusses the application of the confidence region concept to the detection of additive failures relevant to inertial navigation systems. Willsky and Jones (1976) discuss adaptive filtering and its application to the detection of additive failures in linear systems. Caglayan (1980) establishes conditions for detectability of additive jump failures in linear systems. Nash *et al* (1971) use optimal smoothing to model step, ramp and other additive disturbances to gyroscopic inertial navigation systems. Baruh uses a modal method to detect actuator (1986) and sensor (1987) failures in distributed systems. Massoumnia and Vander Velde (1988) use a parity-check technique to diagnose sensor and actuator failures in linear systems.

A primary challenge in diagnosing a malfunction arises from the uncertainty in the form and properties of the failure. Determination of the best possible malfunction diagnosis capability depends on modelling the failure uncertainty. A set-theoretic, rather than probabilistic, representation of uncertainty in the failure is employed in this work. This approach is motivated by the lack of detailed probabilistic information on the possible failures. Set theoretical representations of uncertainty have been employed in a wide range of engineering applications. Schweppe (1968, 1973), Bertsekas and Rhodes (1971), Witsenhausen (1968a,b), Schmitendorf (1987), Tempo (1988) and others have used unknown-but-bounded set theoretic models to represent uncertain inputs in the control and estimation of linear systems. Ben-Haim (1986, 1989) has represented uncertain malfunctions in dynamical systems with a set-theoretical approach. Ben-Haim (1985) has used set models of uncertainty in the optimal design of assay systems for measuring spatially random material. Ben-Haim and Elias (1987) have represented uncertainty in inverse heat transfer measurements with sets of spatially varying heat transfer coefficients. Ben-Haim and Elishakoff (1989) have described geometric imperfections in thin shells using sets of imperfection functions. Common to all these treatments of uncertainty is the fact that *convex sets* of functions characterize the uncertain temporally and/or spatially varying quantity. This approach will be succintly referred to as *convex modelling.*

A multitude of powerful concepts for failure diagnosis has been developed, but a comprehensive methodology for designing diagnosis algorithms is lacking. One component in an overall design analysis is the determination of the best diagnosis capability which can be attained by any state space algorithm. The *benchmark diagnosis* developed in this report does precisely that for additive failures in a linear deterministic dynamic system.

A common approach to malfunction diagnosis is based on hypothesizing a set of possible malfunctions, and then subjecting measurements of the system to a maximum likelihood test, in order to decide which hypothesized malfunction is most likely to have given rise to the measurements. This approach is appealing for several reasons. The concept of maximum likelihood is intuitively satisfying as a criterion of optimality. In addition, prior information about the system can be exploited by judicious selection of the hypothesized malfunctions.

The performance of a multi-hypothesis algorithm for malfunction diagnosis is limited by the disparity between its finite set of hypothesized malfunctions and the infinity of possible failures. A large number of hypothesized malfunctions is usually deemed necessary for reliable diagnosis in the presence of the substantial uncertainty which accompanies the occurrence of failures. However, real-time implementation of a multi-hypothesis algorithm of high multiplicity is problematical. The second concept developed in this report *multi-hypothesis distinguishability* provides a method for evaluating the performance of a multi-hypothesis algorithm with respect to failure uncertainty. This performance-evaluation forms the basis for selecting a robust and efficient collection of hypothesized malfunctions.

3 Normal Dynamics and Control of the AFTI/F16

3.1 Formulation of the Normal Dynamics

The representation of the dynamics of the AFTI/F16 aircraft is based on data presented by Schneider (1986). The dynamics for steady-state linearized flight are presented in state space form as:

$$\frac{dx}{dt} = Ax + Bu \tag{1}$$

where x is an 8-dimensional state vector, u is a 6-dimensional control vector, and A and B are constant dynamics and control matrices. The 8 state variables are: pitch angle, forward velocity, angle of attack, pitch rate, bank angle, sideslip angle, roll rate and yaw rate. The 6 control variables are: right and left horizontal tails (elevators), right and left wing flaps, canards (operated symmetiically) and rudder. The structure of matrices A and B are reproduced in tables 1 and 2.

3.2 Formulation of an Automatic Controller

An automatic controller has been formulated for the linear dynamic model described in the previous subsection. The aim of the controller is to restore the state variables to nearly zero values, by applying control proportional to the state. The duration of the control period is fixed, and denote as t_f. The feedback gain is chosen so as to minimize the integrated state-variable deviations from zero, to minimize the integrated control, and to minimize the magnitude of the final state variables. Specifically, the control is required to minimize the following expression:

$$J = (x^T S_f x)_{t_f} + \int_0^{t_f} \left(x^T R x + u^T V u \right) \, dt \tag{2}$$

With this formulation it can be shown (Bryson and Ho, 1975, p 148-53), that the control vector is given by:

$$u(t) = -V^{-1} B^T S(t) x(t) \tag{3}$$

where the gain matrix, $S(t)$, must satisfy the following differential matrix Riccati equation:

$$\frac{dS}{dt} = -SA - A^T S + SBV^{-1} B^T S - R \tag{4}$$

with the endpoint boundary condition: $S(t_f) = S_f$.

3.3 Numerical Demonstration of the Normal Dynamics

The dynamical behavior of the AFTI/F16 aircraft model employed in this project is briefly demonstrated in this section. Open-loop and closed-loop flight is presented. In the open-loop mode one of the control variables is fixed at a non-zero value, while the others are all fixed at zero. The dynamic behavior is calculated from eq.(1). In the closed-loop mode the flight is initiated as in the open-loop mode: with one fixed non-zero control function. The time-dependent controller is actuated as soon as any of the state variables exceeds a preset threshold value.

0	0	0	1.00000	0	0	0	0
−32.1830	0.012075	38.2906	−30.1376	0	0	0	0
−0.00112	−0.000022	−1.48446	0.994789	0	0	0	0
−0.000309	−0.00013	4.27171	−0.777221	0	0	0	0
0	0	0	0	0	0	1.00000	0
0	0	0	0	0.03449	−0.343554	0.0326360	−0.997556
0	0	0	0	0	−55.2526	−2.80004	0.145674
0	0	0	0	0	7.23700	−0.0231840	−0.362530

Table 1: The Matrix A. The units of the state variables are radians, radians/sec or feet/sec (after Schneider, (1986)).

0	0	0	0	0	0
1.00296	1.00296	1.15840	1.15840	0	0
−0.0746135	−0.0746135	−0.122462	−0.122462	0	0
−12.0291	−12.0291	−3.23635	−3.23635	0	0
0	0	0	0	0	0
0.0133045	−0.0133045	−0.0006855	0.0006855	0.0267340	0.0370320
−25.3645	25.3645	−25.5251	25.5251	5.53185	10.3955
−2.56855	2.56855	−0.625030	0.625030	5.89254	−5.80890

Table 2: The Matrix B. The units of the state and control variables are radians, radians/sec or feet/sec (after Schneider, (1986)).

Symbol	State Variable	Control Variable
octagon	pitch	right elevator
Δ	forward velocity	left elevator
$+$	angle of attack	right wing flap
$\times$	pitch rate	left wing flap
diamond	roll	canard
$\uparrow$	yaw	rudder
table	roll rate	—
Z	yaw rate	—

Table 3: Legend for figures in this section.

The controller is operated for the duration of $t_f = 0.15$ seconds. At the end of this control period the control actuators are all fixed at their last values, and the flight is continued in open-loop (fixed control) mode until a state variable again exceeds the threshold value. The controller is again imposed, and so on. The values of the matrices A and B are given in tables 1 and 2 (from Schneider, (1986)).

Figures 1 - 4 show open loop behavior of the aircraft at 0.9 Mach and 20,000 feet altitude. These four figures show the time dependence of the 8 state variables in response to four different fixed-control conditions. The units are feet, seconds and degrees. The single non-zero control function is fixed at +4 degrees in each case. In figure 1 the non-zero control is the right horizontal tail (otherwise known as the right elevator); the right flap in Figure 2; the canards (operated symmetrically) in Figure 3; and the rudder in Figure 4. The legend of the symbols for the figures in this section appears in table 3.

The open-loop dynamics have been calculated from eq.(1) by a simple finite-difference method. The Riccati equation, relation (4), must be solved for the closed-loop calculation. This is done by a backward finite difference calculation. Then eq.(1) is solved, together with eq.(3), by finite difference. The time step size for all finite difference calculations is 0.001 second. The matrices S_f and R in

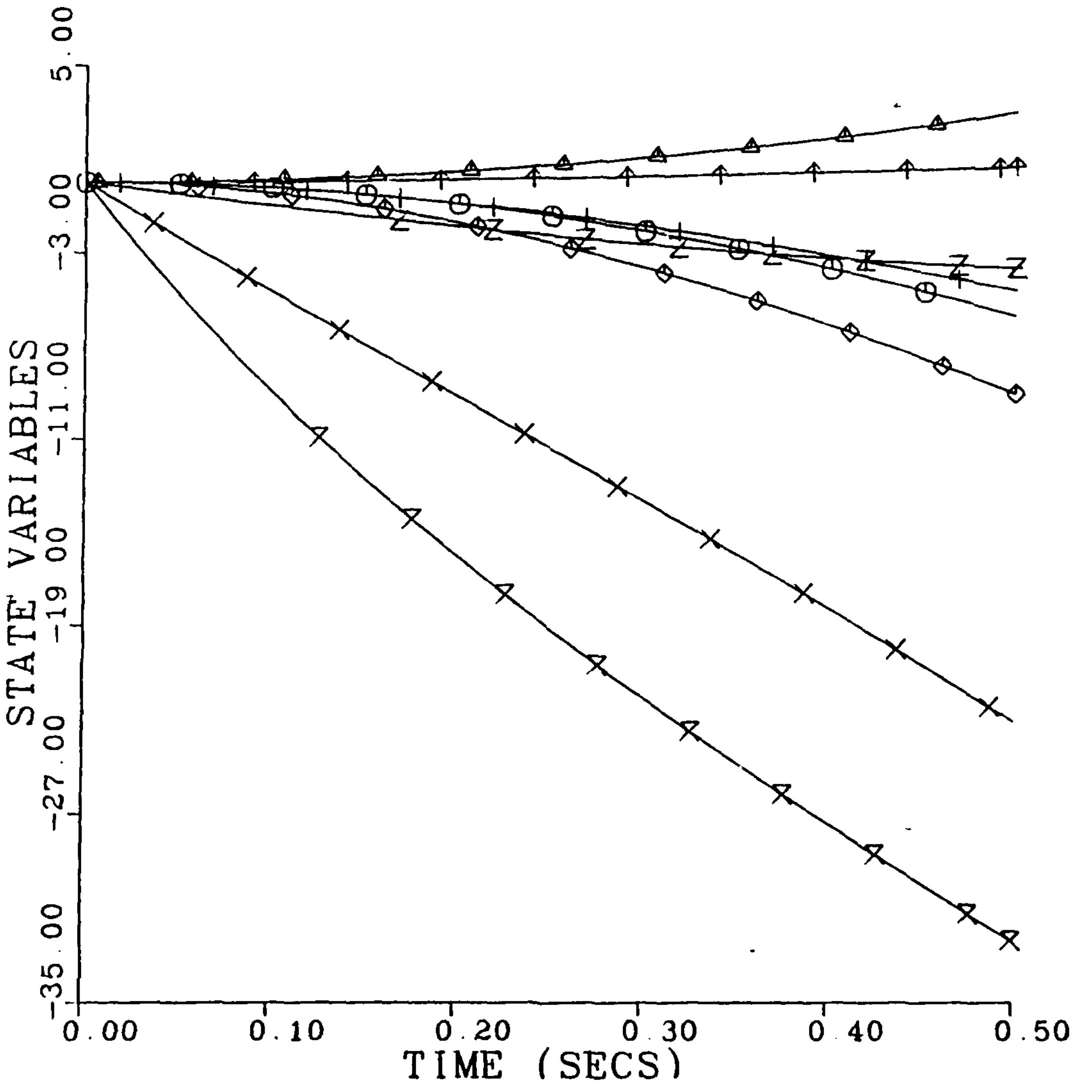

Figure 1: Dynamic open-loop response to a +4 degree deflection of the right elevator.

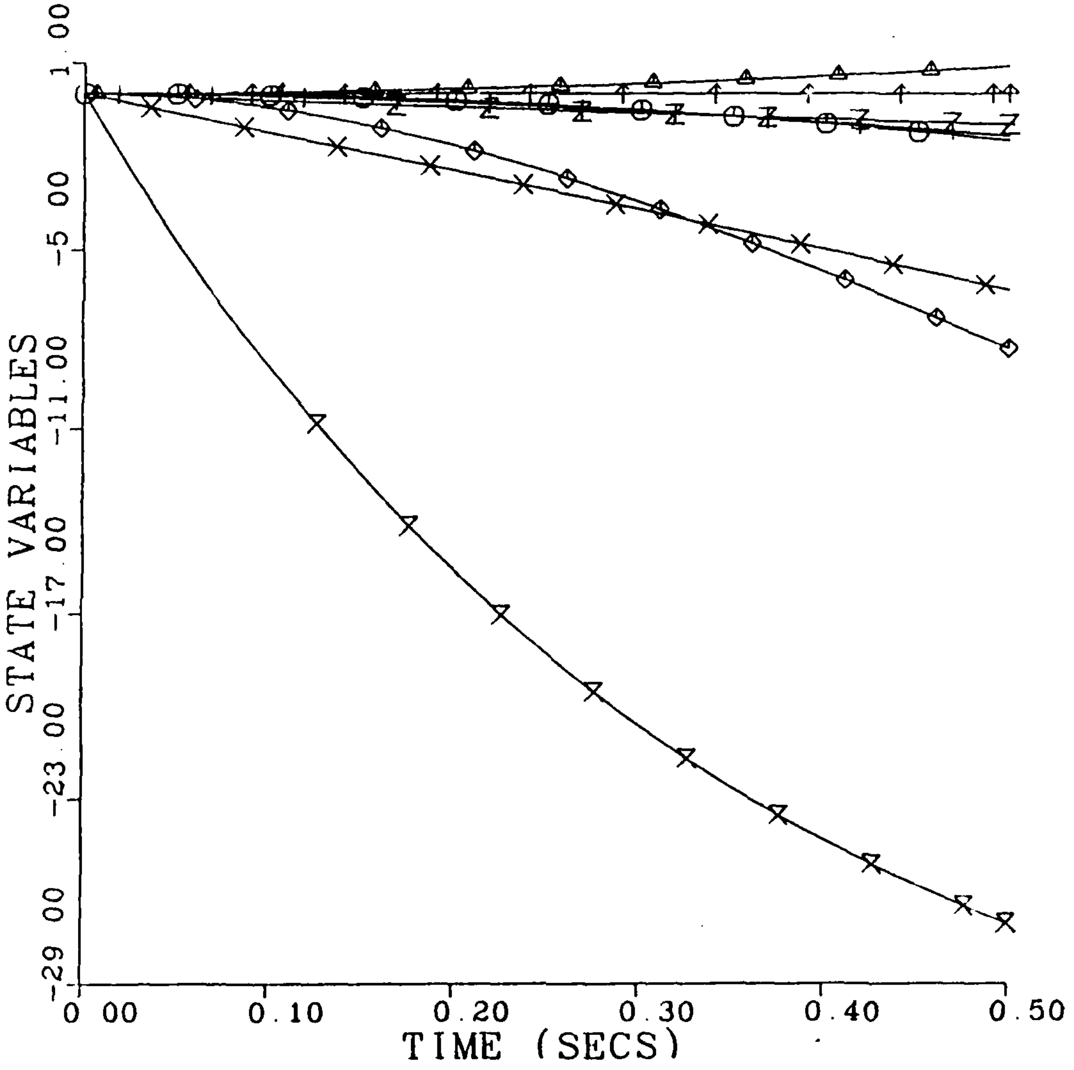

Figure 2: Dynamic open-loop response to a +4 degree deflection of the right wing flap.

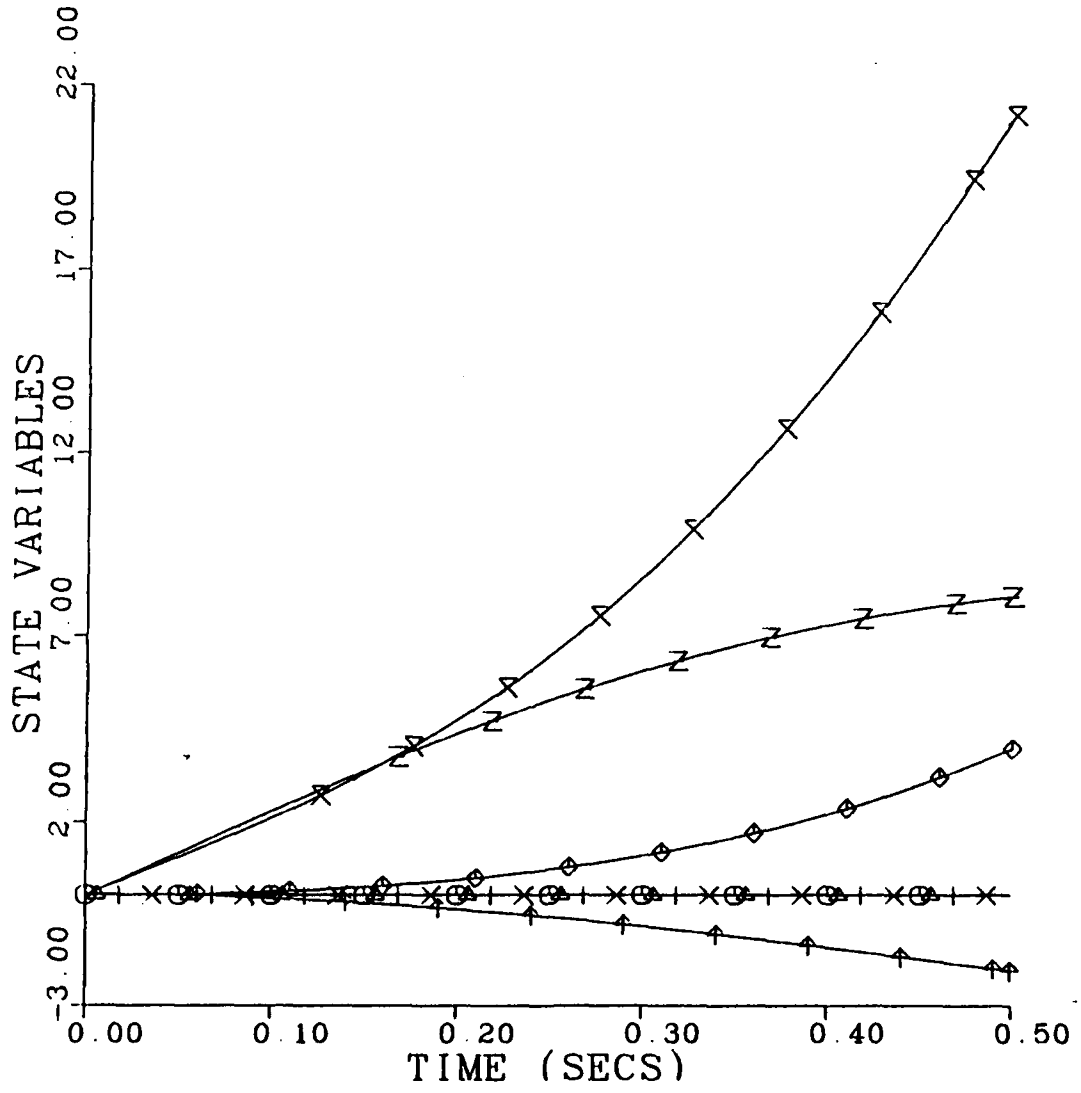

Figure 3: Dynamic open-loop response to a +4 degree symmetrical deflection of the canards.

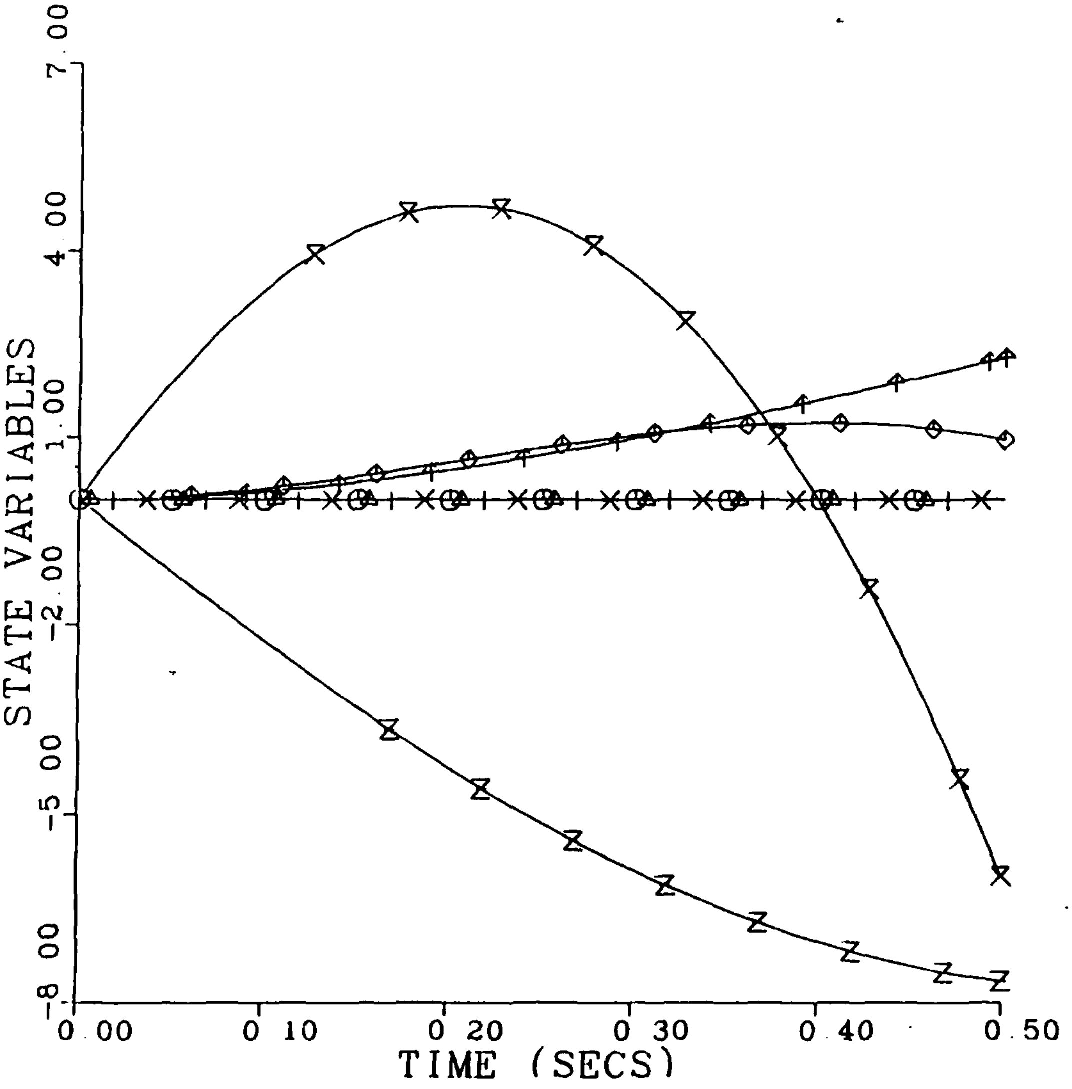

Figure 4: Dynamic open-loop response to a +4 degree deflection of the rudder.

the Riccati equation are positive semi-definite while V is positive definite. In the numerical calculations to be discussed, these matrices are chosen to be diagonal, with equal diagonal elements. The diagonal elements of R equal $50/t_f$, of V equal $2/t_f$ and of S_f equal 0.25.

Figures 1 and 2 show substantial similarity in the effect of the right wing flap and the right elevator. In each, a +4 degree deflection results in appreciable roll rate: about -30 degrees/sec at the end of 0.5 second. The elevator produces more pitching motion than the wing flap. The other state variables are less affected during the first 0.5 second.

Figure 3 shows the dynamic response to a +4 degree symmetrical deflection of the canards. The roll and yaw motions are strongly induced, while the longitudinal state variables are completely unaffected.

Figure 4 demonstrates the response to a +4 degree deflection of the rudder. The yawing moment is predominant, and the rolling moment is pronounced and reverses its sign after about 0.4 second. The longitudinal state variables are unaffected.

Figures 5 – 12 show the state and control variables in four different closed-loop modes. As explained above, each flight is initiated in the open-loop mode with a single non-zero control held at a fixed value of +4 degrees. (This initial value of the control is not depicted in the figures because it is far off scale. Rather, all the control variables are shown as initially equal to zero). In figures 5 and 6 the non-zero control function is the right elevator; in figures 7 and 8 the right wing flap; in figures 9 and 10 the canards; in figures 11 the rudder.

Figure 5 shows the dynamic, closed-loop response to an initial +4 degree deflection of the right elevator. Rolling and pitching moments develop quickly, as in figure 1. However, after only 5 milliseconds, the absolute value of the roll rate exceeds the threshold of 0.5 for triggering the controller. The controller is actuated, as seen in figure 6, for 0.15 second, during which time the rolling and pitching moments are rapidly reduced. This is achieved by positive deflections of canards and the rudder, and negative deflections of the right wing flap and the left and right elevators. The left wing flap varies from positive to negative values. After completion of the 0.15 second control period, the control functions are fixed at their last values and the flight is continued in the open-loop (fixed-control) mode.

Figures 7 and 8 show the response and controls when the initial fixed-control perturbation was a +4 degree deflection of the right wing flap. The dynamic and control responses are qualitatively similar to those shown in response to an initial right elevator deflection.

Figures 9 and 10 show the dynamic and control responses to a +4 degree deflection of the canards. Strong rolling and yawing moments develop quickly, as in figure 3. This results in actuation of the controller after 0.022 seconds. Positive right flap and elevator, positive rudder and symmetrical negative left flap and elevator, together with negative deflection of the canards, result in reversal of the lateral moments. Note, however, that the control period terminates (at 0.172 second) before the yawing and rolling moments are completely zeroed. In the fixed-control period a negative yaw rate develops, resulting in re-activation of the controls at 0.471 second.

Figures 11 and 12 show the dynamic and control responses to an initial positive deflection of the rudder.

4 Representing Control-Actuator Failure

Our aim in this section is to develop a convenient formalism for representing the measurements of a linear system with control actuator failure.

The dynamic behavior and measurements of the failure-free linear deterministic system are represented as:

$$\begin{aligned} \frac{dx}{dt} &= A(t)x(t) + B(t)u(t) && (5) \\ y(t) &= G(t)x(t) && (6) \end{aligned}$$

where x, y and u are state, measurement and control vectors of dimensions N, L

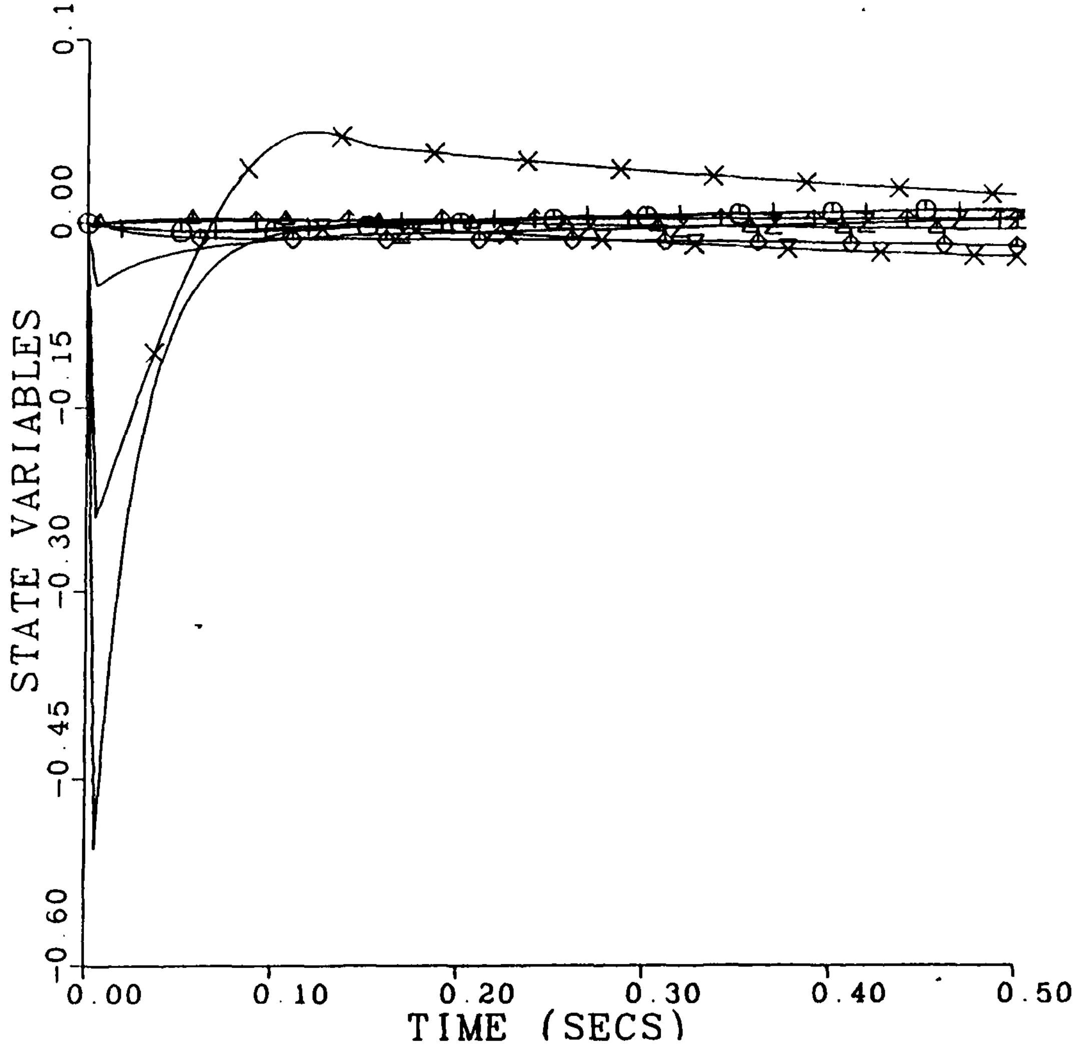

Figure 5: Dynamic closed-loop response to a +4 degree deflection of the right elevator.

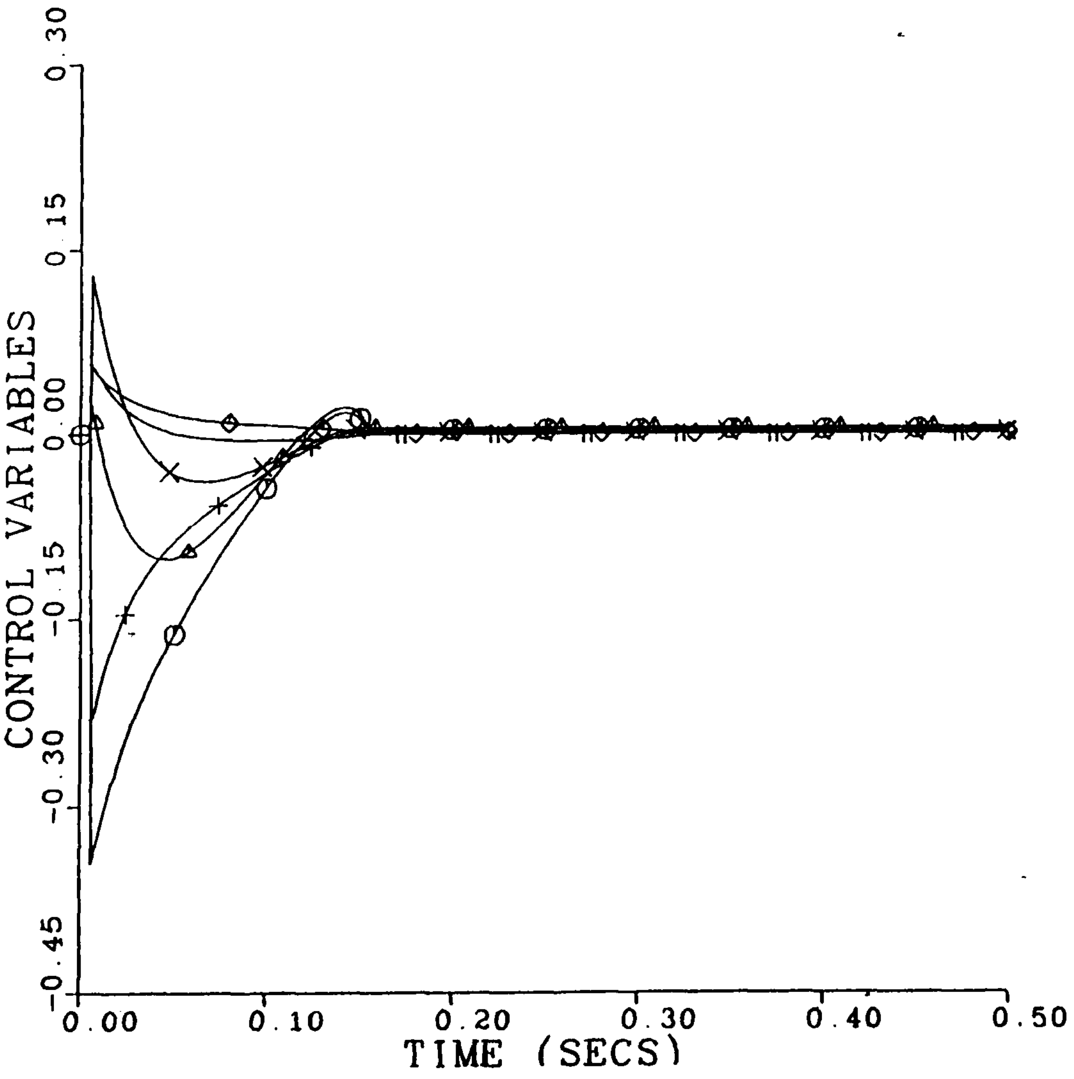

Figure 6: Automatic control variables in response to a +4 degree deflection of the right elevator.

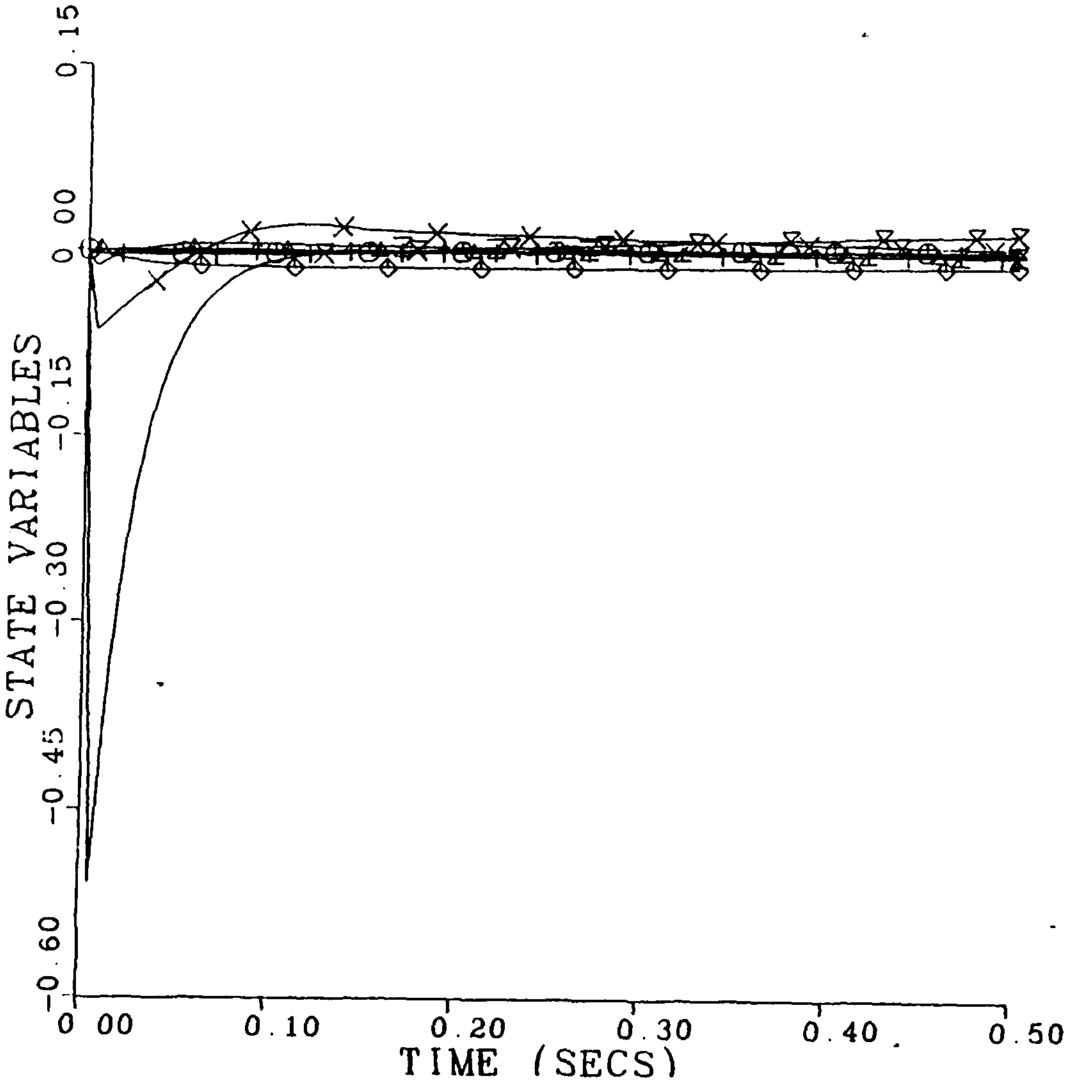

Figure 7: Dynamic closed-loop response to a +4 degree deflection of the right wing flap.

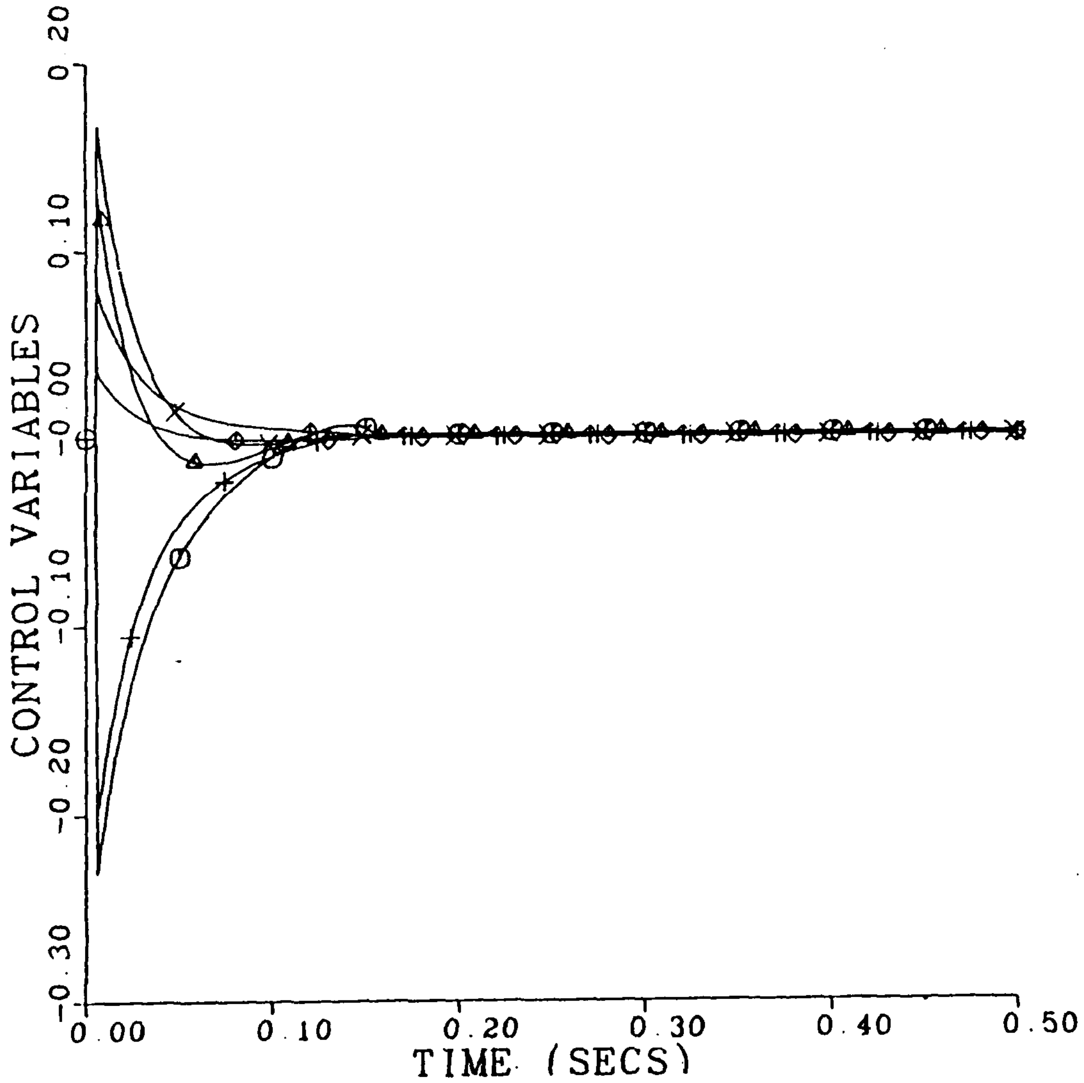

Figure 8: Automatic control variables in response to a +4 degree deflection of the right wing flap.

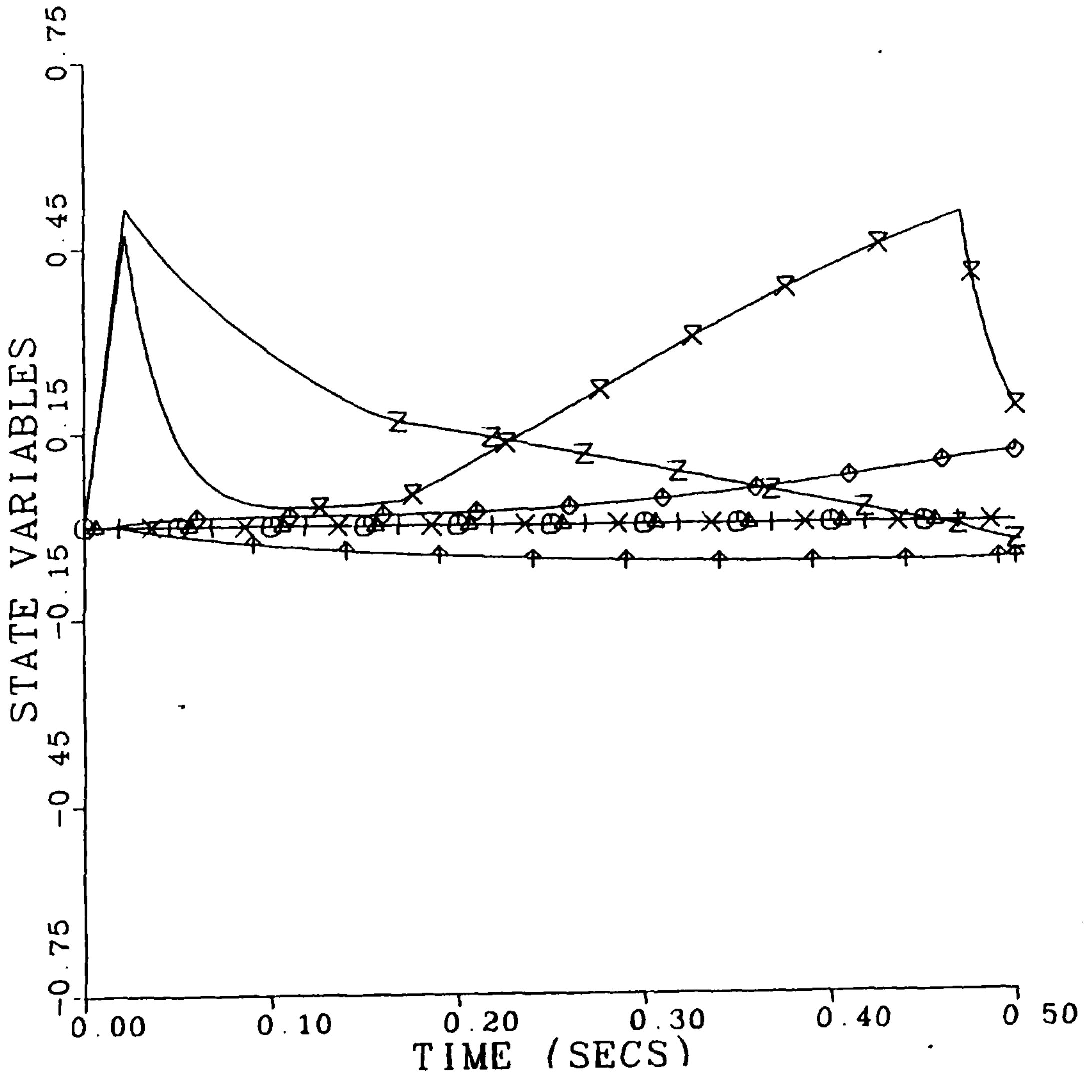

Figure 9: Dynamic closed-loop response to a +4 symmetrical degree deflection of the canards.

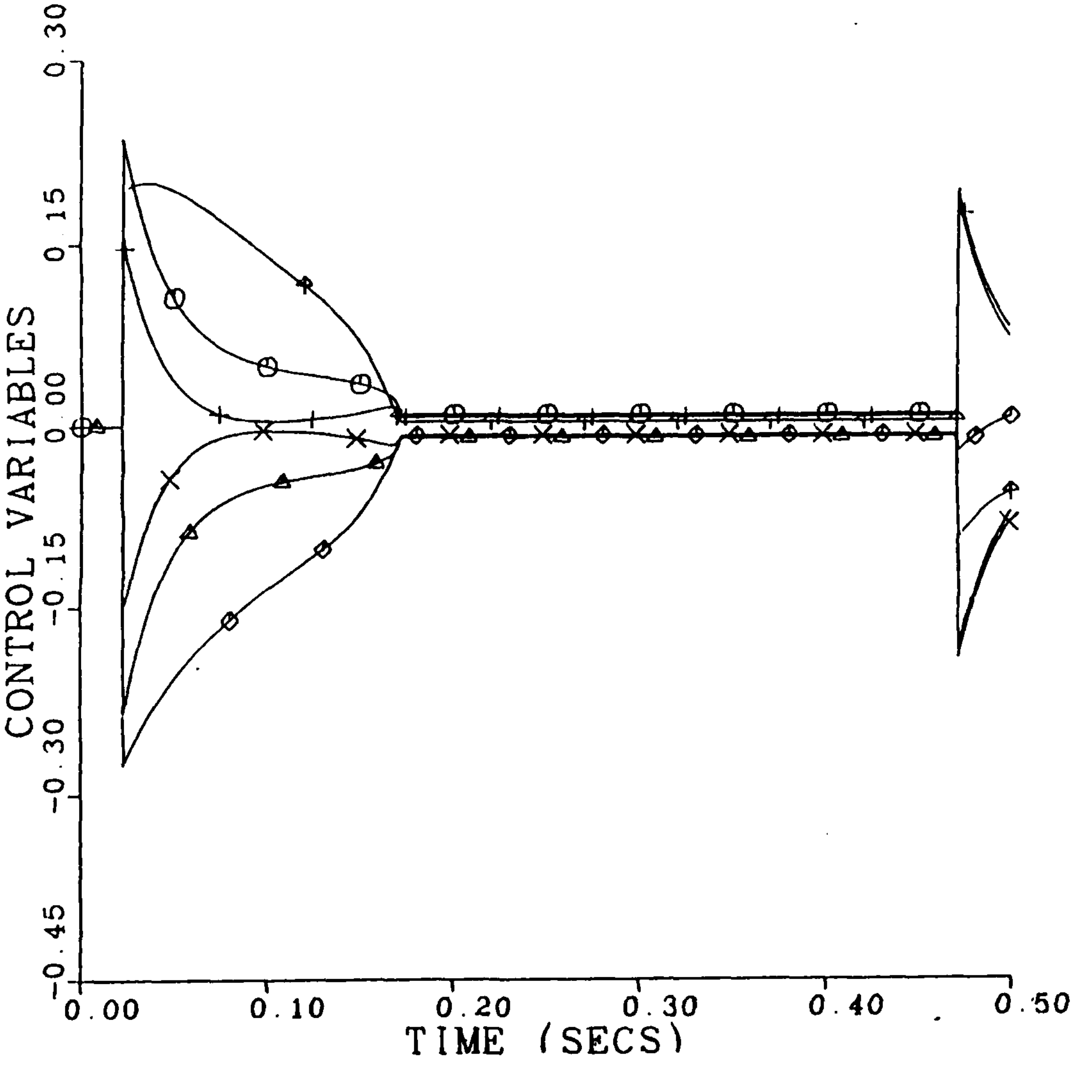

Figure 10: Automatic control variables in response to a +4 symmetrical degree deflection of the canards.

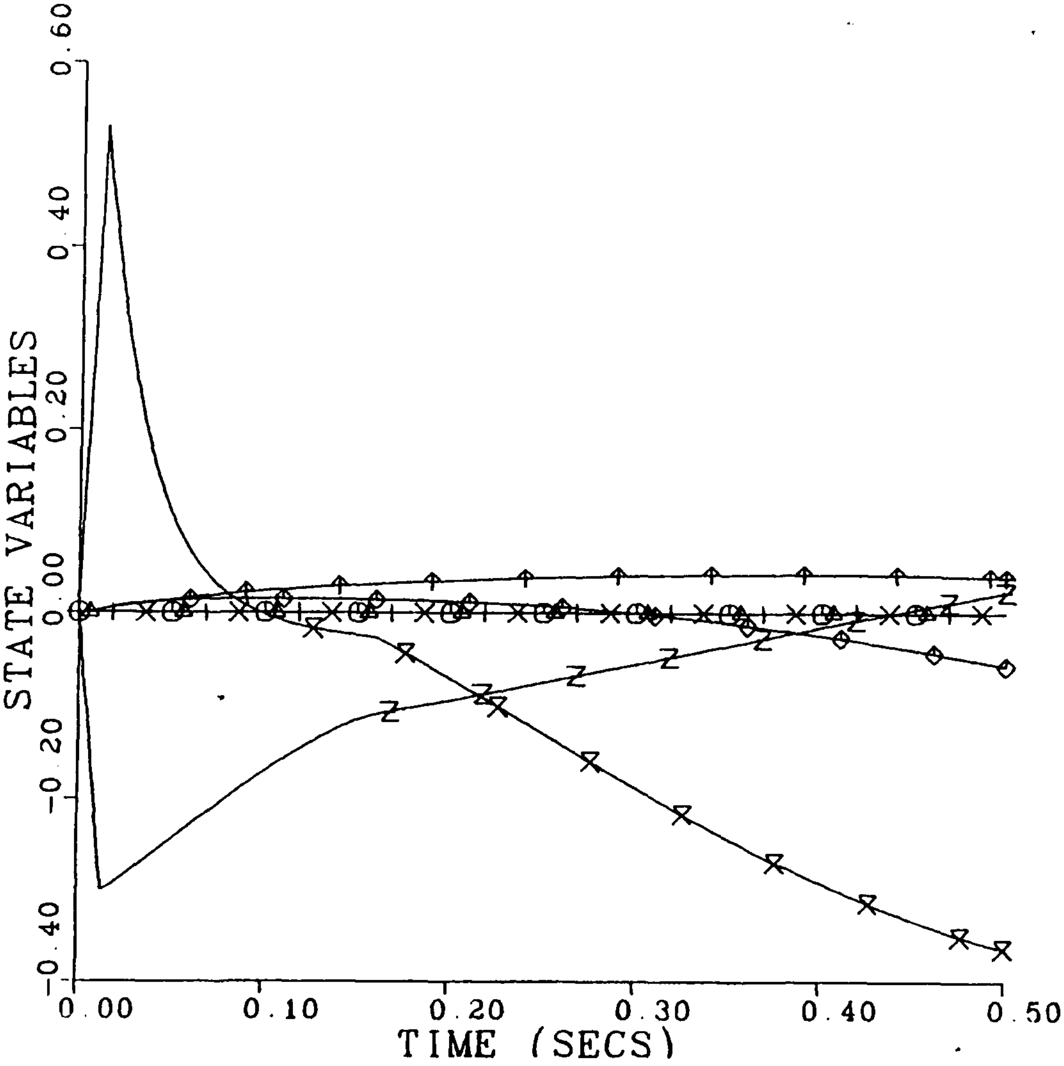

Figure 11: Dynamic closed-loop response to a +4 degree deflection of the rudder.

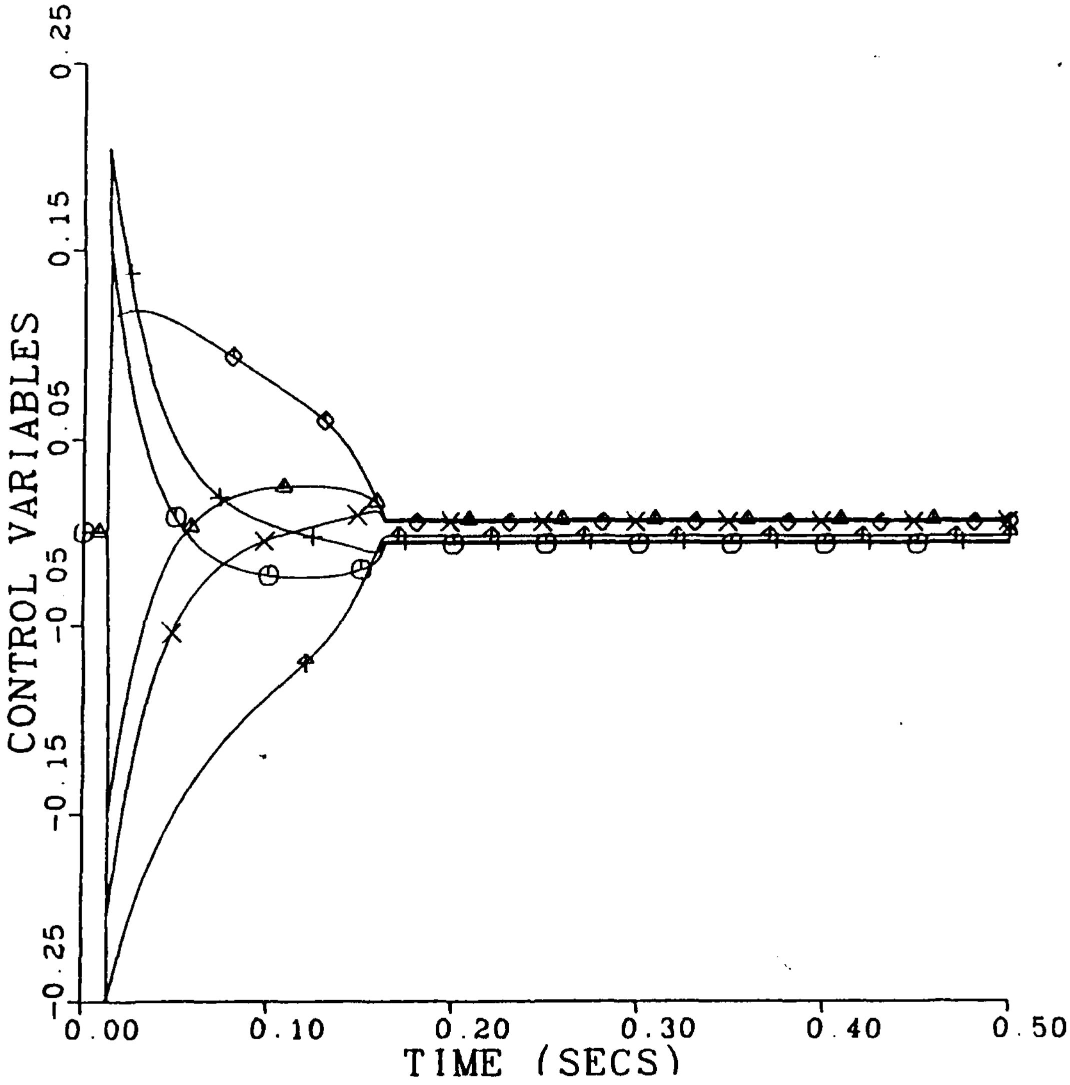

Figure 12: Automatic control variables in response to a +4 degree deflection of the rudder.

and M respectively and A, B and G are known matrices. The system is regulated automatically by a feedback controller proportional to the state:

$$u(t) = S(t)x(t) \tag{7}$$

Let us now consider the representation of J control actuator failures. The indices of the failed actuators are $\mathbf{j} = (j_1, \ldots, j_J)$. When a malfunction occurs in the j_kth control actuator its normal control function, $u_{j_k}(t)$, is replaced by an autonomous expression, $f_{j_k}(t)$. Let $f(t)$ be an M-element vector whose j_kth element is the autonomous behavior of the failed j_kth actuator, for $k = 1, \ldots, J$, and whose other elements are zero. Let $I_{\mathbf{j}}$ be the matrix obtained from the $M \times M$ identity matrix by removing each of the J rows $j_1, \ldots, j_J$. Thus $I_{\mathbf{j}}u(t)$ is a vector of length $M - J$ obtained by removing the elements $j_1, \ldots, j_J$ from the nominal control vector, $u(t)$. Similarly, $BI_{\mathbf{j}}^T$ is an $N \times (M - J)$ matrix obtained by removing the columns $j_1, \ldots, j_J$ from the matrix B. (The superscript T denotes n atrix transposition.) Using this notation, the dynamic response of the system to failure of J actuators whose indices are $\mathbf{j}$ is described by:

$$\frac{dx}{dt} = A(t)x(t) + B(t)I_{\mathbf{j}}^T I_{\mathbf{j}}u(t) + B(t)f(t) \tag{8}$$

The normal algorithm still calculates the feedback control vector from eq.(7). However, f_{j_k} is implemented rather than $u_{j_k}(t)$. Combining eqs. (7) and (8) yields:

$$\frac{dx}{dt} = \left[A(t) + B(t)I_{\mathbf{j}}^T I_{\mathbf{j}}S(t)\right] x(t) + B(t)f(t) \tag{9}$$

The state vector $x(t)$ can be expressed in terms of a transition matrix $X_{\mathbf{j}}$, which is the solution of the following differential equation (Bellman, 1974):

$$\frac{dX_{\mathbf{j}}}{dt} = \left[A(t) + B(t)I_{\mathbf{j}}^T I_{\mathbf{j}}S(t)\right] X_{\mathbf{j}}(t) \quad , \quad X_{\mathbf{j}}(0) = I \tag{10}$$

Finally, the measurement vector in response to failure vector $f(t)$ is:

$$y_f(t) = G(t)X_{\mathbf{j}}(t)x(0) + G(t)\int_0^t X_{\mathbf{j}}(t)X_{\mathbf{j}}^{-1}(\tau)B(\tau)f(\tau)\,d\tau \tag{11}$$

5 Convex Models of Malfunction Uncertainty

The satisfactory diagnosis of malfunction depends upon prior knowledge of the malfunction phenomenon as a whole. However, malfunction is often so complex that one is unable to formulate a probability measure, defined in a space of failure functions, which expresses the probability density for occurrence of specific malfunctions. On the other hand, partial information is likely to enable the characterization of possible malfunctions in set-theoretic terms.

In a set-theoretic model of malfunction the failure vector $f(t)$ belongs to a set of malfunctions which all share some global, phenomenological property in common. For example, one may consider failure sets of step-like functions which occur at or around a particular time, or ramp-like functions all with similar slopes. Alternatively, the failure-functions may be uniformly bounded and of extended duration, or may be transient disturbances of bounded total energy.

In general, the *failure set* $F(p)$, where p is a parameter vector, is the set of vector-valued functions which represent all realizable failures of type p. It is often found in practice that the information available for characterizing the possible malfunctions leads naturally to assuming $F(p)$ to be a convex set. We shall assume our failure sets to be convex, and refer to $F(p)$ as a *convex model* for failures of type p. The adoption of a convex model for representing the variability of each type of failure can be motivated by theoretical considerations. This is briefly discussed in the Appendix.

A widely used convex model for set-theoretic representation of uncertainty is based on assuming that the functions in question are uniformly bounded. The failure sets are defined as:

$$\begin{aligned} F(p) \;=\; & \{f^T = (f_1, \ldots, f_M) : \; \tilde{p}_m \le f_m(t) \le \hat{p}_m \;, \\ & t \in [0, \infty) \;, \; m = 1, 2, \ldots, M\} \end{aligned} \tag{12}$$

where $p = (\tilde{p}_1, \hat{p}_1, \ldots, \tilde{p}_M, \hat{p}_M)$. Thus the autonomous (malfunctioning) value of the

mth control function varies arbitrarily between $\tilde{p}_m$ and $\hat{p}_m$. Usually the number of actuator failures is less than the dimension M of the control vector. This is represented by choosing $\tilde{p}_m = \hat{p}_m = 0$ for each of the functioning actuators.

Eq. (11) maps each failure vector $f(t)$ in $F(p)$ to a vector $y_f(t)$ in measurement space. Let $C(p)$ be the set of all the measurement vectors obtained from failures in the set $F(p)$. That is:

$$C(p) = \{y : \ y(t) = y_f(t) \quad \text{for all} \quad f \in F(p)\} \tag{13}$$

We will call $C(p)$ the ***complete response set*** for failures of type p.

6 Benchmark Diagnosis Capability

6.1 The Concept of Benchmark Diagnosis

Malfunction diagnosis[1] is based on distinguishing between response sets which correspond to distinct types of failure. Response sets which are far apart will be easily distinguished, while malfunction diagnosis becomes more difficult and uncertain for response sets which are closer together. Finally, if two response sets $C(p)$ and $C(q)$ overlap, then no algorithm will be able to distinguish every occurrence of failure of type p from every occurrence of failure-type q. The capability for malfunction diagnosis is thus ultimately limited by the overlapping of response sets. The disjointness of response sets determines the limiting or ***benchmark*** malfunction diagnosis capability. This benchmark is an expression of the failure uncertainty characteristic of the system studied, of the failure environment within which it operates, and of the knowledge embodied in the system and failure models. Improved malfunction diagnosis can be obtained only by modifying the system or its measurements or the failure environment, or by augmenting the knowledge with which the system and its failures are modelled.

[1] The material of this section will be presented at the IFAC Conference on Advanced Information Processing in Automatic Control, 3 – 5 July 1989, Nancy, France. (Ben-Haim, 1989a).

If the complete response sets for two types of failures are disjoint we will say that the failures are ***benchmark distinguishable***, meaning that it is possible, in principle, to distinguish between all occurrences of these failure types. On the other hand, failure types whose response sets intersect are said to be ***benchmark indistinguishable***, indicating that no algorithm can distinguish between every possible occurrence of these failure types. Determination of the benchmark diagnosis capability thus involves establishing the disjointness or intersection of response sets.

The disjointness of response sets, and hence the benchmark diagnosis capability, is readily formulated by using a hyperplane separation theorem for convex sets (Rockafellar, 1970). Let $C(p)$ and $C(q)$ be non-empty, closed and bounded convex response sets in a finite dimensional Euclidean space. $C(p)$ and $C(q)$ are disjoint if and only if there exists a hyperplane P such that $C(p)$ is in one half-space defined by P and $C(q)$ is in the other half-space. This theorem can be expressed algebraically as follows:

$$C(p) \cap C(q) = \emptyset \tag{14}$$

if and only if there exists a real vector ω such that:

$$\max_{c \in C(p)} \omega^T c < \min_{d \in C(q)} \omega^T d \tag{15}$$

For further discussion of relations 14 and 15 see Ben-Haim, 1985.

The disjointness of complete response sets is established by determining the extremal values on the complete response sets of the linear function $\omega^T x$. The complete response sets $C(p)$ and $C(q)$ are images of the failure sets $F(p)$ and $F(q)$, as in eq. (13). Consequently, a necessary and sufficient condition for the disjointness of $C(p)$ and $C(q)$ is the existence of a vector ω such that:

$$\max_{\phi \in F(p)} \omega^T y_\phi < \min_{\psi \in F(q)} \omega^T y_\psi \tag{16}$$

This relation forms the basis for an algorithmic determination of the disjointness of response sets. The algorithm searches for a vector ω which satisfies relation

(16). (It is sufficient to search on the unit sphere because (16) is homogeneous in ω.) Disjointness is established if such a vector is found. If no such vector exists, then the sets intersect. In this way the benchmark malfunction diagnosis capability of the system can be determined.

6.2 Hyperplane Separation for Uniformly Bounded Malfunctions

The benchmark diagnosis capability is based on determining the disjointness of complete response sets for different types of failure. Each complete response set $C(p)$ is the image in measurement space of the set $F(p)$ of possible failures of type p. The failure set $F(p)$ represents the uncertainty in the realization of failures of type p. In this section we develop the hyperplane separation algorithm for determining the disjointness of complete response sets for uniformly bounded actuator failures.

Consider two different failure sets: $F(p)$ represents the failure of J control actuators whose indices are $\mathbf{j} = (j_1, \ldots, j_J)$ and with uniform bounds $p = (\tilde{p}_1, \hat{p}_1, \ldots, \tilde{p}_M, \hat{p}_M)$ on the failure functions. $F(q)$ represents the failure of K actuators whose indices are $\mathbf{k} = (k_1, \ldots, k_K)$ with uniform bounds $q = (\tilde{q}_1, \hat{q}_1, \ldots, \tilde{q}_M, \hat{q}_M)$ on the failure functions. The corresponding complete response sets are $C(p)$ and $C(q)$, as defined by eq. (13). Our aim is to determine whether or not there exists a vector ω satisfying relation (16).

Let $X_{\mathbf{j}}(t)$ and $X_{\mathbf{k}}(t)$ represent the transition matrices for the two types of failure, obtained as solutions of eq. (10). Note that the transition matrix depends on which actuators have failed, but is entirely independent of the uniform bounds on the failed actuators. For convenience of notation define $\lambda^m(t, \tau)$ and $\mu^m(t, \tau)$ as the mth columns of $G(t)X_{\mathbf{j}}(t)X_{\mathbf{j}}^{-1}(\tau)B(\tau)$ and $G(t)X_{\mathbf{k}}(t)X_{\mathbf{k}}^{-1}(\tau)B(\tau)$, respectively. Also denote $y_{\mathbf{j}}^o(t) = G(t)X_{\mathbf{j}}(t)x(0)$ and $y_{\mathbf{k}}^o(t) = G(t)X_{\mathbf{k}}(t)x(0)$.

Using this notation one finds that, for an arbitrary $\phi \in F(p)$, the inner product

$\omega^T y_\phi$ assumes the form:

$$\omega^T y_\phi = \omega^T y_{\mathbf{j}}^o(t) + \sum_{m=1}^{M} \int_0^t \phi_m(\tau)\omega^T \lambda^m(t,\tau)\, d\tau \tag{17}$$

Likewise, for an arbitrary element $\psi \in F(q)$, the inner product $\omega^T y_\psi$ becomes:

$$\omega^T y_\psi = \omega^T y_{\mathbf{k}}^o(t) + \sum_{m=1}^{M} \int_0^t \psi_m(\tau)\omega^T \mu^m(t,\tau)\, d\tau \tag{18}$$

Examination of eq. (17) shows that $\omega^T y_\phi$ achieves its maximum when each $\phi_m(\tau)$ is chosen to switch between its extremal values as $\omega^T \lambda^m(t,\tau)$ changes sign. Specifically, $\omega^T y_\phi$ is maximized by choosing the elements of ϕ as:

$$\phi_m(\tau) = \begin{cases} \hat{p}_m & , \quad \omega^T \lambda^m(t,\tau) \geq 0 \\ \tilde{p}_m & , \quad \omega^T \lambda^m(t,\tau) < 0 \end{cases} \tag{19}$$

Let D_{m+} and D_{m-} denote the subsets of $[0,t]$ for which $\omega^T \lambda^m(t,\tau)$ is non-negative and negative, respectively. Thus:

$$\max_{\phi \in F(p)} \omega^T y_\phi = \omega^T y_{\mathbf{j}}^o(t) + \sum_{m=1}^{M} \left[\hat{p}_m \int_{D_{m+}} \omega^T \lambda^m(t,\tau)\, d\tau + \tilde{p}_m \int_{D_{m-}} \omega^T \lambda^m(t,\tau)\, d\tau \right] \tag{20}$$

Similarly, $\omega^T y_\psi$ in eq. (18) is minimized by choosing each $\psi_m(\tau)$ as a switching function which follows the sign changes of $\omega^T \mu^m(t,\tau)$. Let Δ_{m+} and Δ_{m-} denote the subsets of $[0,t]$ for which $\omega^T \mu^m(t,\tau)$ is non-negative and negative, respectively. Thus:

$$\min_{\psi \in F(q)} \omega^T y_\psi = \omega^T y_{\mathbf{k}}^o(t) + \sum_{m=1}^{M} \left[\tilde{q}_m \int_{\Delta_{m+}} \omega^T \mu^m(t,\tau)\, d\tau + \hat{q}_m \int_{\Delta_{m-}} \omega^T \mu^m(t,\tau)\, d\tau \right] \tag{21}$$

Relations (20), (21) and (16) together define a necessary and sufficient condition for the disjointness of $C(p)$ and $C(q)$, and hence for the benchmark distinguishability of the corresponding failure sets.

6.3 Example: Actuator Failures in AFTI/F16 Aircraft

The benchmark malfunction diagnosis capability has been evaluated for a range of uniformly bounded control actuator failures in the AFTI/F16 aircraft in steady rectilinear flight at 0.9 Mach and 20,000 feet altitude. The 8 state variables are: pitch angle, forward velocity, angle of attack, pitch rate, bank angle, sideslip angle, roll rate and yaw rate. The 6 control variables are: right and left horizontal tails (elevators), right and left wing flaps, canards (operated symmetrically) and rudder. The dynamics, control and measurement matrices A, B and G are constant in time. The values of the matrices A and B presented in tables 1 and 2 (from Schneider (1986)) and G is the identity matrix.

The system is controlled by an automatic regulator whose aim is to restore the state variables to nearly zero values by applying minimal control proportional to the state. The duration of the control period is fixed, and denoted as t_f. The controller minimizes the following expression:

$$J = (x^T S_f x)_{t_f} + \int_0^{t_f} \left(x^T R x + u^T V u\right) dt \tag{22}$$

With this formulation it can be shown (Bryson and Ho, 1975) that the control vector is given by:

$$u(t) = -V^{-1} B^T S(t) x(t) \tag{23}$$

where the gain matrix, $S(t)$, must satisfy the following differential matrix Riccati equation:

$$\frac{dS}{dt} = -SA - A^T S + SBV^{-1}B^T S - R \tag{24}$$

with the endpoint boundary condition: $S(t_f) = S_f$.

The Riccati equation is solved numerically by backward finite difference calculation. The eq. (5) is solved, together with eq. (23), by finite difference. The time step size for all finite difference calculations is 0.001 second. The matrices S_f, R and V are diagonal, with equal diagonal elements. The diagonal elements of R

equal $50/t_f$, of V equal $2/t_f$ and of S_f equal 0.25. The duration of the control period is $t_f = 0.15$ sec.

Let us consider two failure sets. One set, $F(p)$, will be a set of failures in the 2nd and 6th control actuators (left elevators and rudder). Thus:

$$p = (0,\ 0,\ \tilde{p}_2,\ \hat{p}_2,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ \tilde{p}_6,\ \hat{p}_6) \qquad (25)$$

We will choose:

$$\tilde{p}_2 = \tilde{p}_6 = 1^o \quad , \quad \hat{p}_2 = \hat{p}_6 = 2^o \qquad (26)$$

Thus $F(p)$ represents all failures in which the deflection of the left elevator and the rudder vary arbitrarily and independently between 1^o and 2^o, while all the remaining actuators vary according to the nominal feedback controller.

The second failure set, $F(q)$, is a set of failures in the 2nd and 5th control actuators (left elevators and canards). Thus:

$$q = (0,\ 0,\ \tilde{q}_2,\ \hat{q}_2,\ 0,\ 0,\ 0,\ 0,\ \tilde{q}_5,\ \hat{q}_5, 0,\ 0) \qquad (27)$$

We will assume that:

$$\hat{q}_2 = \tilde{q}_2 + 1^o \quad , \quad \hat{q}_5 = \tilde{q}_5 + 1^o \qquad (28)$$

Thus $F(q)$ represents all malfunctions in which the deflection of the left elevator varies between $\tilde{q}_2$ and $\tilde{q}_2 + 1^o$, while the canard deflection varies between $\tilde{q}_5$ and $\tilde{q}_5 + 1^o$.

We will use relation (16) to determine what failure sets $F(p)$ and $F(q)$ are benchmark distinguishable, as a function of the values of $\tilde{q}_2$ and $\tilde{q}_5$. The real-time identification of the failure sets must be performed in a very short duration. It is thus of particular interest to determine which subsets of the 8-component measurement vector provide benchmark distinguishability of the failure sets.

Figure 13 shows part of the $\tilde{q}_5$-versus $\tilde{q}_2$ plane. Each point on this plane specifies a value of $\tilde{q}_2$ and of $\tilde{q}_5$ and thus specifies the parameter vector q, defined by eqs.(27) and (28). Thus each point represents a failure set $F(q)$. Those failure

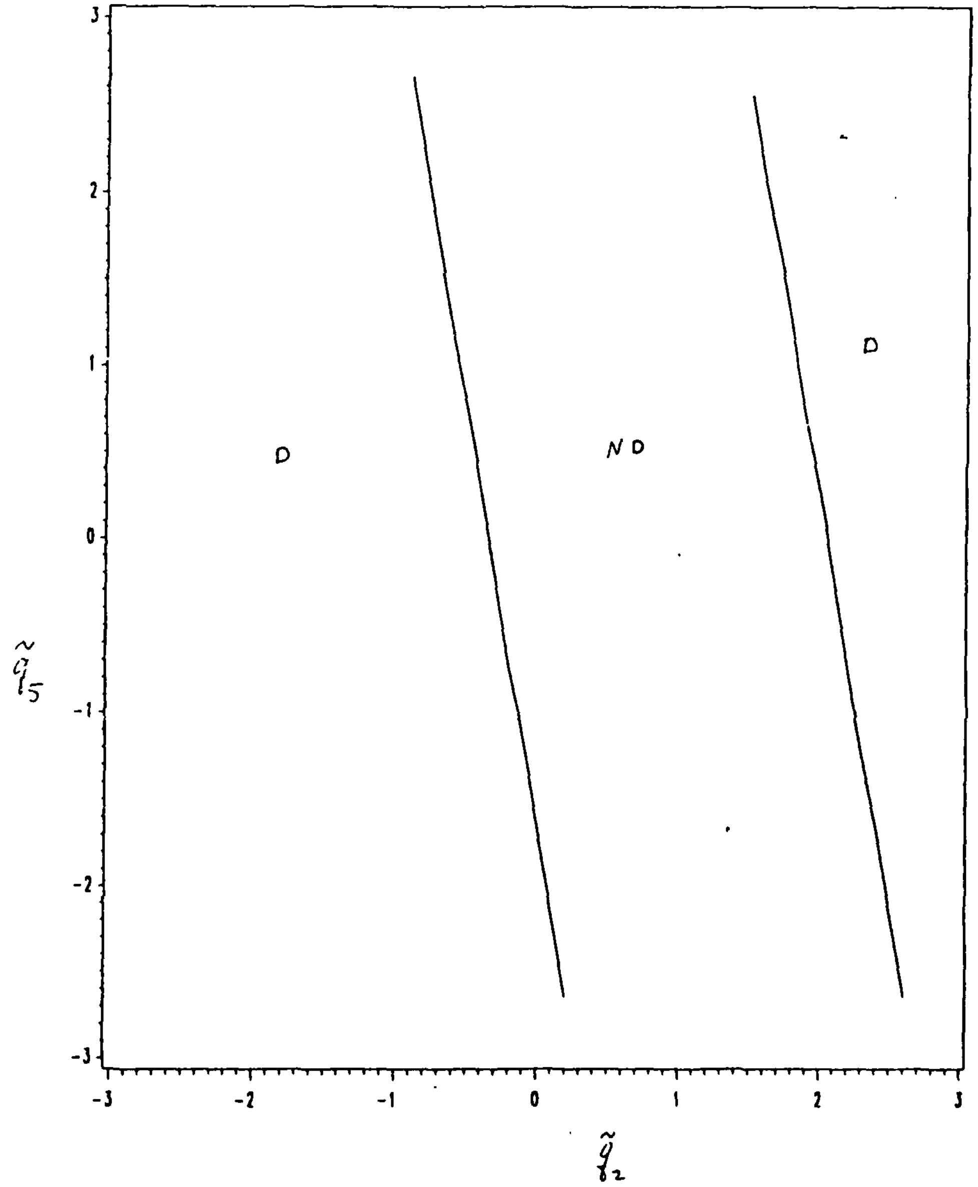

Figure 13: Regions of benchmark distinguishability of $F(q)$ from $F(p)$ for single measurement of the first state variable, pitch angle.

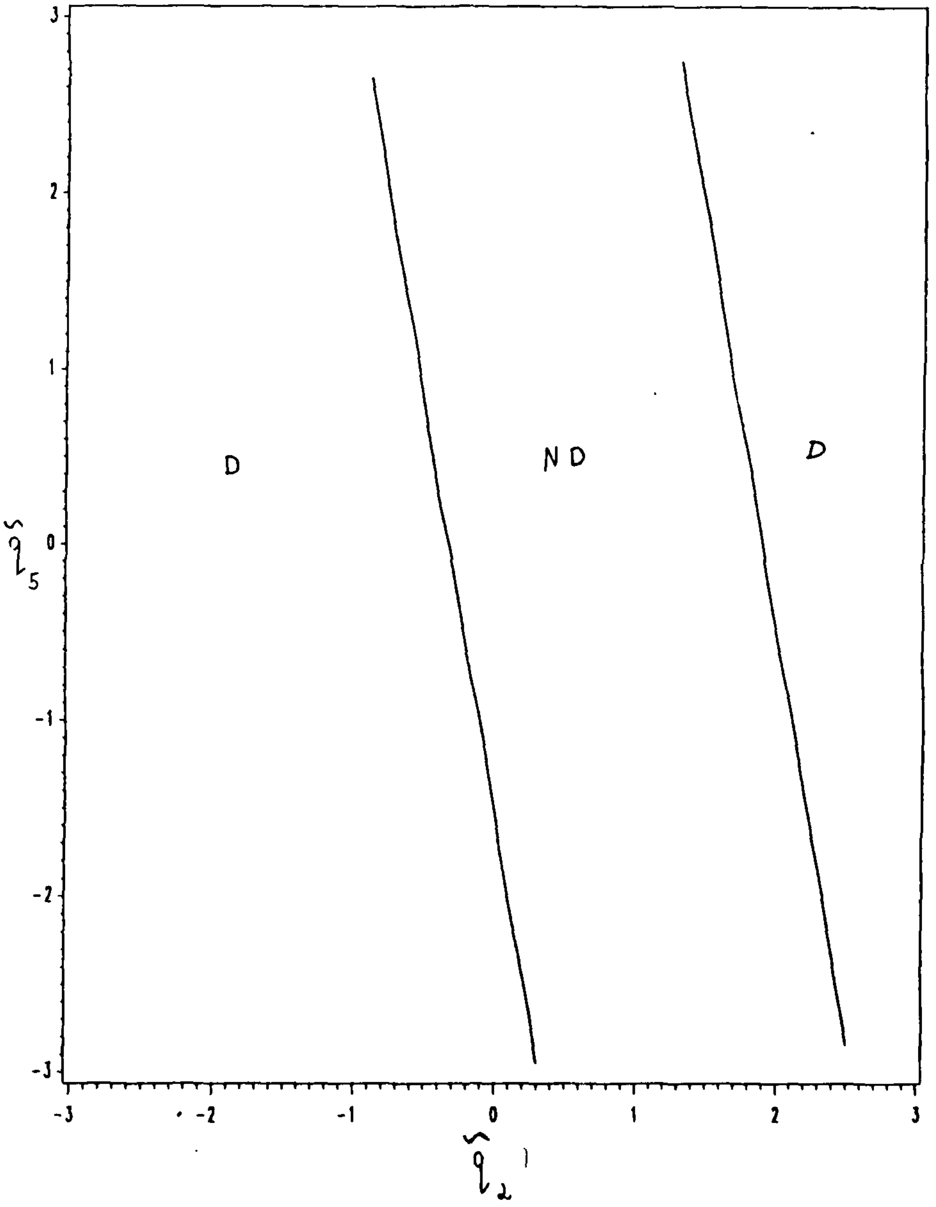

Figure 14: Regions of benchmark distinguishability of $F(q)$ from $F(p)$ for single measurement of the second state variable, forward velocity.

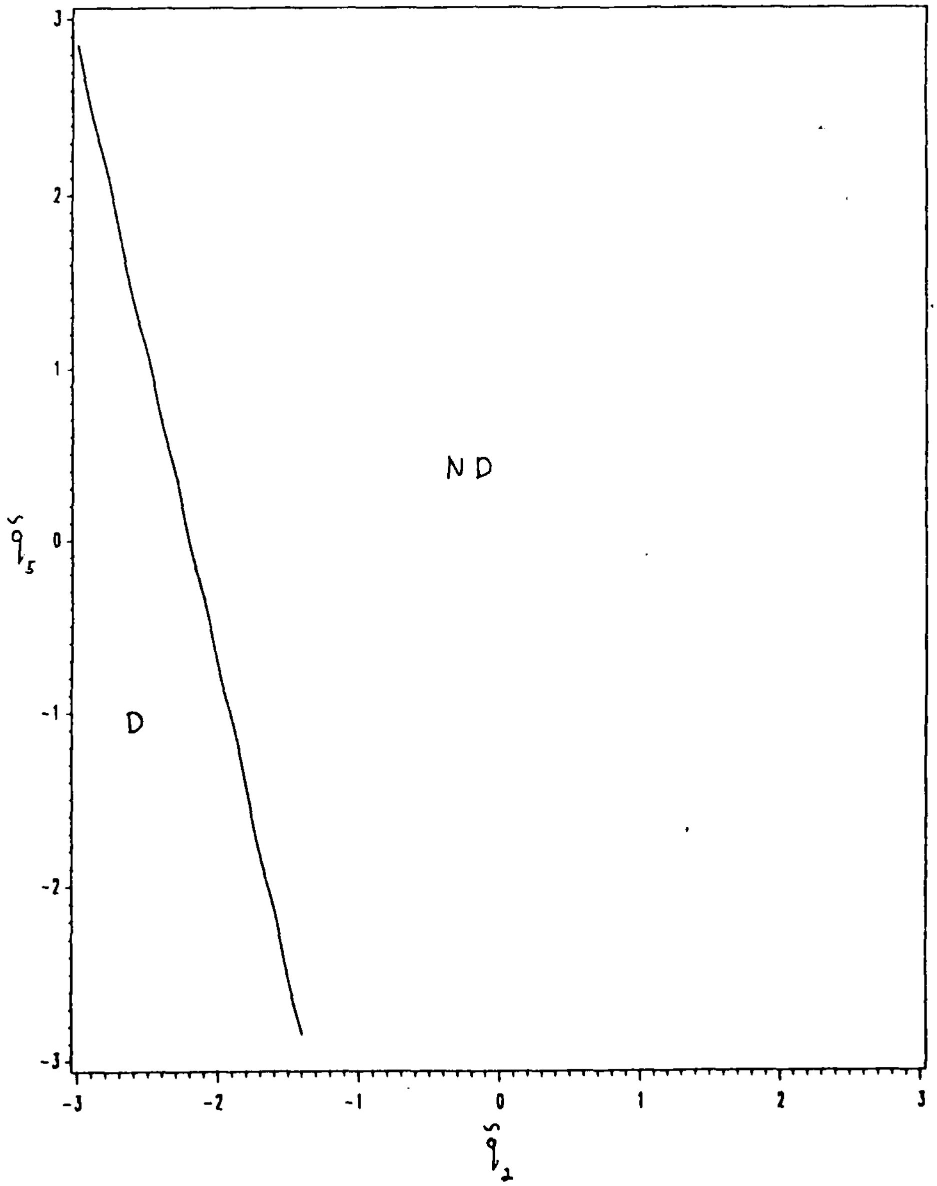

Figure 15: Regions of benchmark distinguishability of $F(q)$ from $F(p)$ for single measurement of the third state variable, angle of attack.

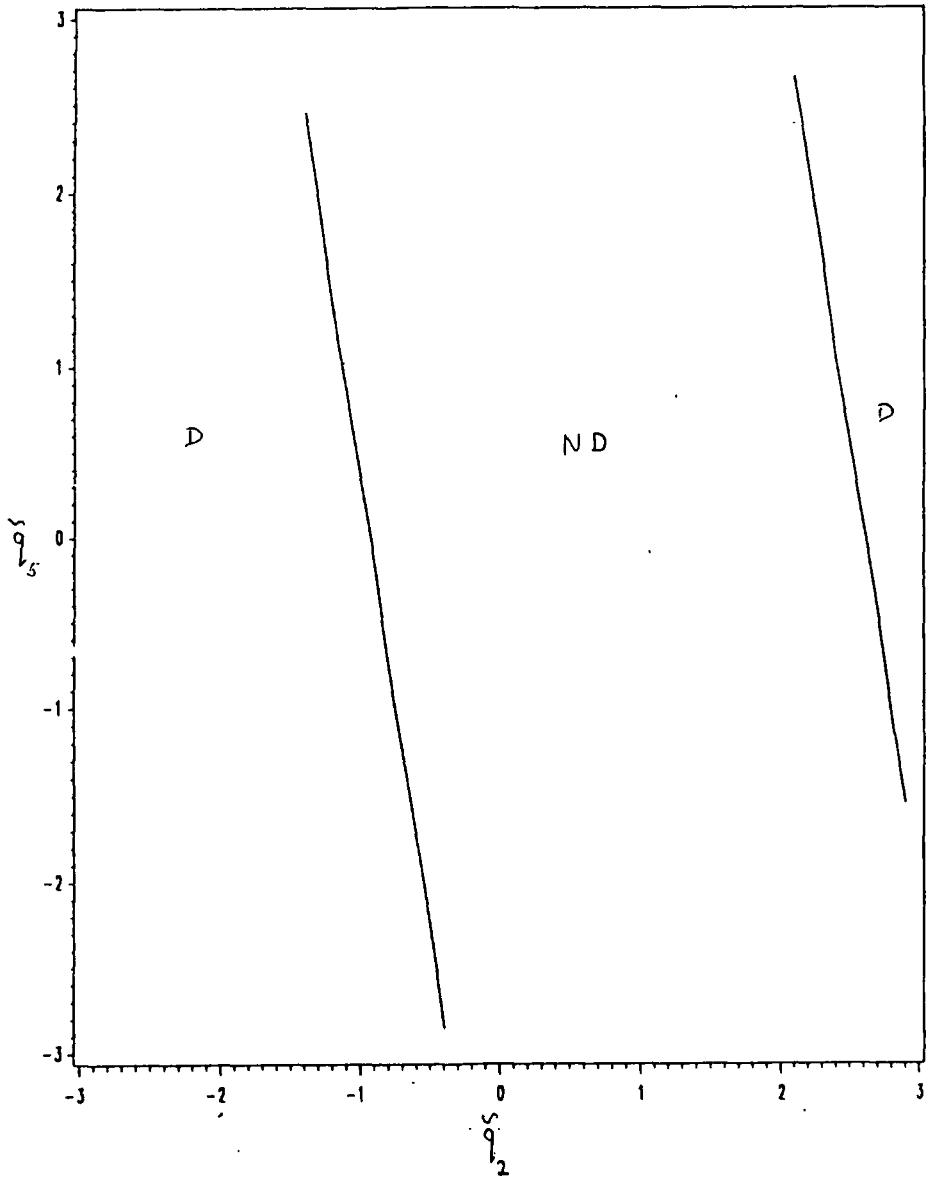

Figure 16: Regions of benchmark distinguishability of $F(q)$ from $F(p)$ for single measurement of the fourth state variable, pitch rate.

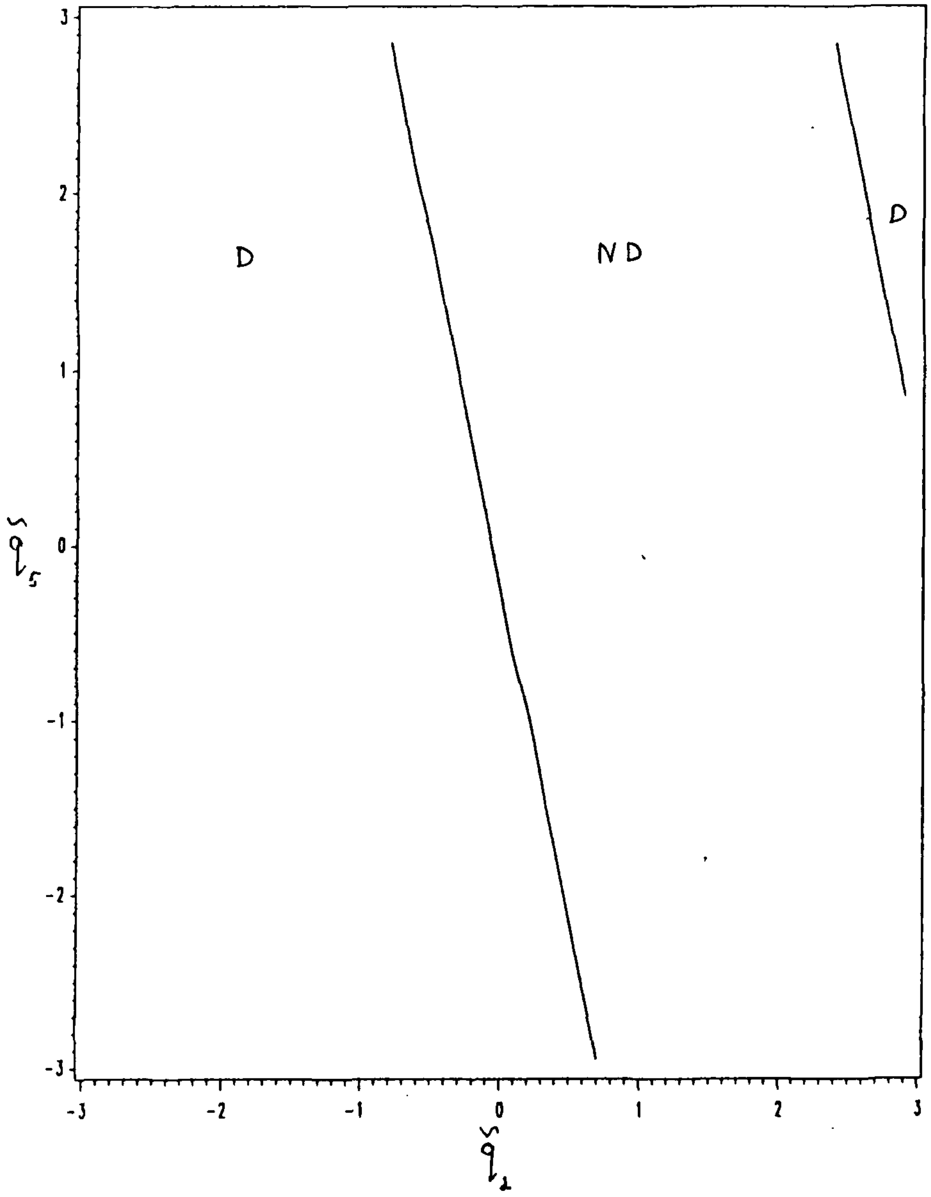

Figure 17: Regions of benchmark distinguishability of $F(q)$ from $F(p)$ for single measurement of the fifth state variable, bank angle.

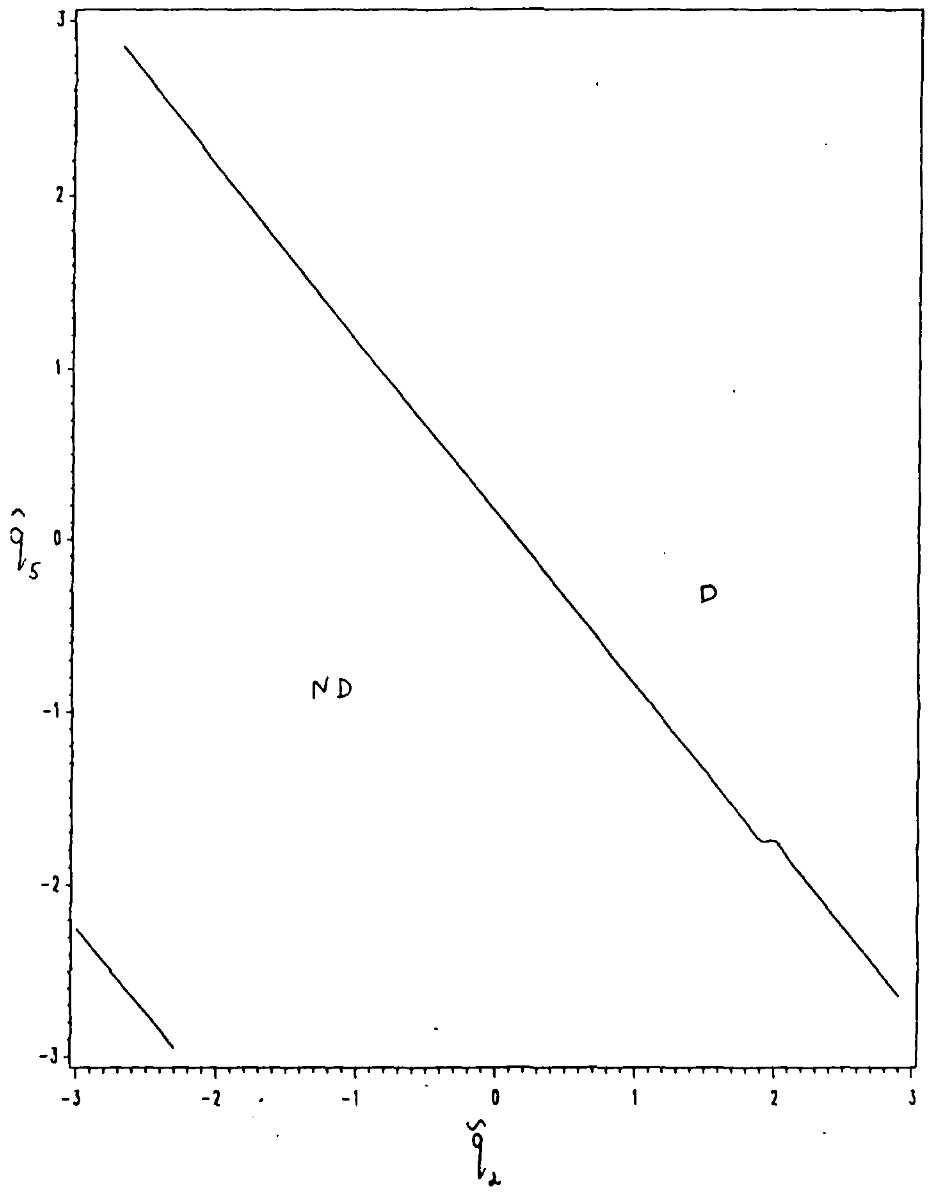

Figure 18: Regions of benchmark distinguishability of $F(q)$ from $F(p)$ for single measurement of the sixth state variable, sideslip angle.

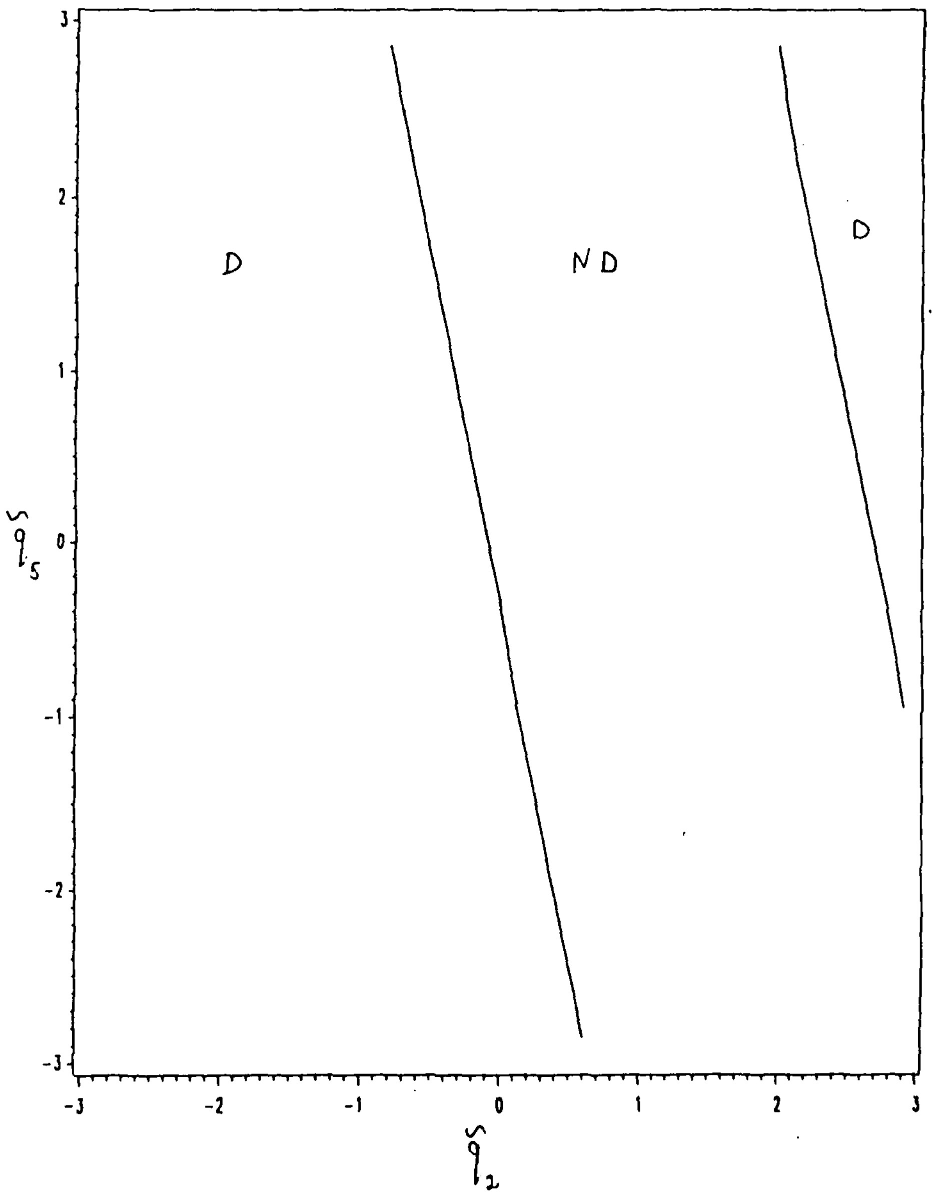

Figure 19: Regions of benchmark distinguishability of $F(q)$ from $F(p)$ for single measurement of the seventh state variable, roll rate.

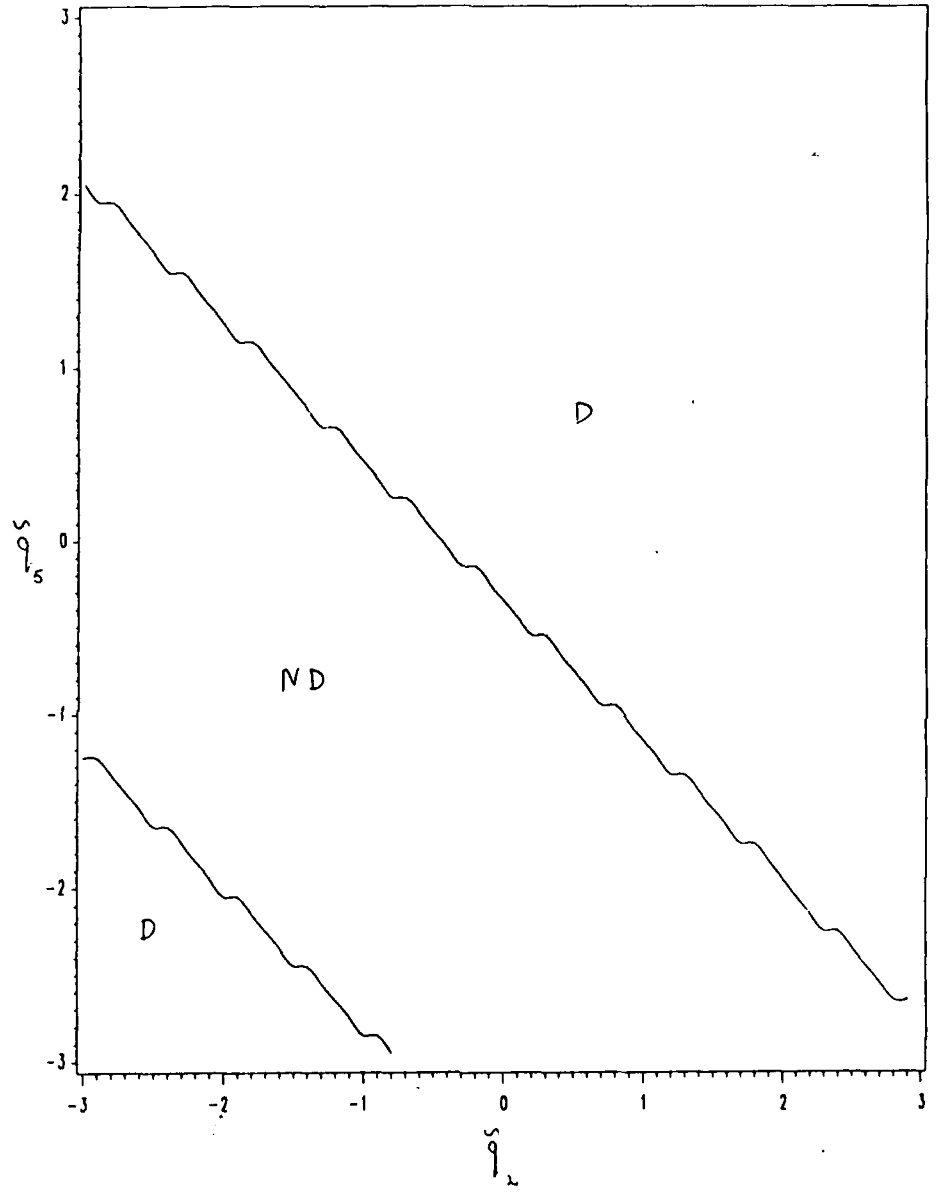

Figure 20: Regions of benchmark distinguishability of $F(q)$ from $F(p)$ for single measurement of the eighth state variable, yaw rate.

sets represented by points in the regions marked 'D' are benchmark distinguishable from the failure set $F(p)$, while those failure sets in the region marked 'ND' are not benchmark distinguishable from $F(p)$, where p is defined by eqs.(25) and (26). Furthermore, this distinguishability is based on measurement of the first state variable alone (pitch angle) 0.15 sec after onset of the failure.

Figures 14 to 20 also portray regions of benchmark distinguishability on the $\tilde{q}_5$ versus $\tilde{q}_2$ plane, for measurement of a single state variable 0.15 sec after onset of failure. The state variables employed in Figures 14 to 20 are: forward velocity, angle of attack, pitch rate, bank angle, sideslip angle, roll rate and yaw rate, respectively. It is seen that the benchmark distinguishability of $F(q)$ from $F(p)$ obtained by measuring any one of the following state variables is approximately the same: 1st, 2nd, 4th, 5th or 7th. On the other hand, measurement of the 6th or 8th state variable provides benchmark distinguishability in a different region of the plane, while measurement of the 3rd state variable provides little distinguishability at all.

It is noted that most of these single-measurement examples provide benchmark distinguishability for roughly half of the range of failure sets $F(q)$ examined. Furthermore, certain pairs of measurements provide complementary distinguishability. For example, the regions of distinghuishability with the 2nd (Figure 14) and the 8th (Figure 20) state variables together nearly cover the entire range of $(\tilde{q}_2, \tilde{q}_5)$ values considered. Figure 21 shows the regions of benchmark distinguishable and non-distinguishable malfunctions based on simultaneous measurement (at $t = 0.15$ sec) of the 2nd and 8th state variables. It is evident that $F(q)$ and $F(p)$ are benchmark distinguishable over most of the values of $(\tilde{q}_2, \tilde{q}_5)$ considered.

Figure 22 shows an overlay of Figures 14 (small dash), 20 (large dash) and 21 (solid). The non-distinguishable region with two measurements is smaller than the intersection of the non-distinguishable regions of the two single measurement cases. Thus simultaneous measurements of two state variables provides better benchmark distinguishability than would be expected from each state variable alone.

A similar phenomenon is observed in Figure 23, which shows the regions of benchmark distinguishablity for simutaneous measurement (at $t = 0.15$ sec) of the 1st (pitch angle) and 6th (sideslip angle) variables (solid line). Figures 13 (large dash) and 18 (small dash) are overlayed for comparison. The non-distinguishable region of the double measurement is smaller than the intersection of the non distinguishable regions of the two single measurements.

However, this mutual improvement is not obtained in every case. Figure 24 shows the benchmark performance of the simultaneous measurement (at $t = 0.15$ sec) of the 2nd (forward velocity) and 7th (roll rate) state variables. In this case the region of two-measurement benchmark distinguishability is precisely the intersection of the two single-measurement regions (Figures 14 and 19).

These examples suffice to demonstrate that relation (16) provides a means of identifying efficient combinations of state variables whose measurement enables reliable, benchmark, differentiation between distinct failure sets.

6.4 Energy-Bounded Failure Functions

The uniform-bound convex model is by far the most widely used set-theoretical representation of uncertainty. It is particularly useful to describe uncertainty with uniform bounds when the failure functions are ***roughly*** constant in time. For instance, the deflection uncertainty of nearly hard failures, wherein the deflections of the failed control surfaces flutter around fixed values, are conveniently represented by uniform bounds. On the other hand, the uncertainty inherent in malfunctions which involve a strong transient component is not conveniently represented with a uniform-bound model. A variety of convex models can be employed for representing the uncertainty in strongly varying malfunctions. In this section we formulate one such model and derive the hyperplane separation criterion for benchmark distinguishability of these sets of failures.

The energy-bound convex model of failure uncertainty is formulated as follows.

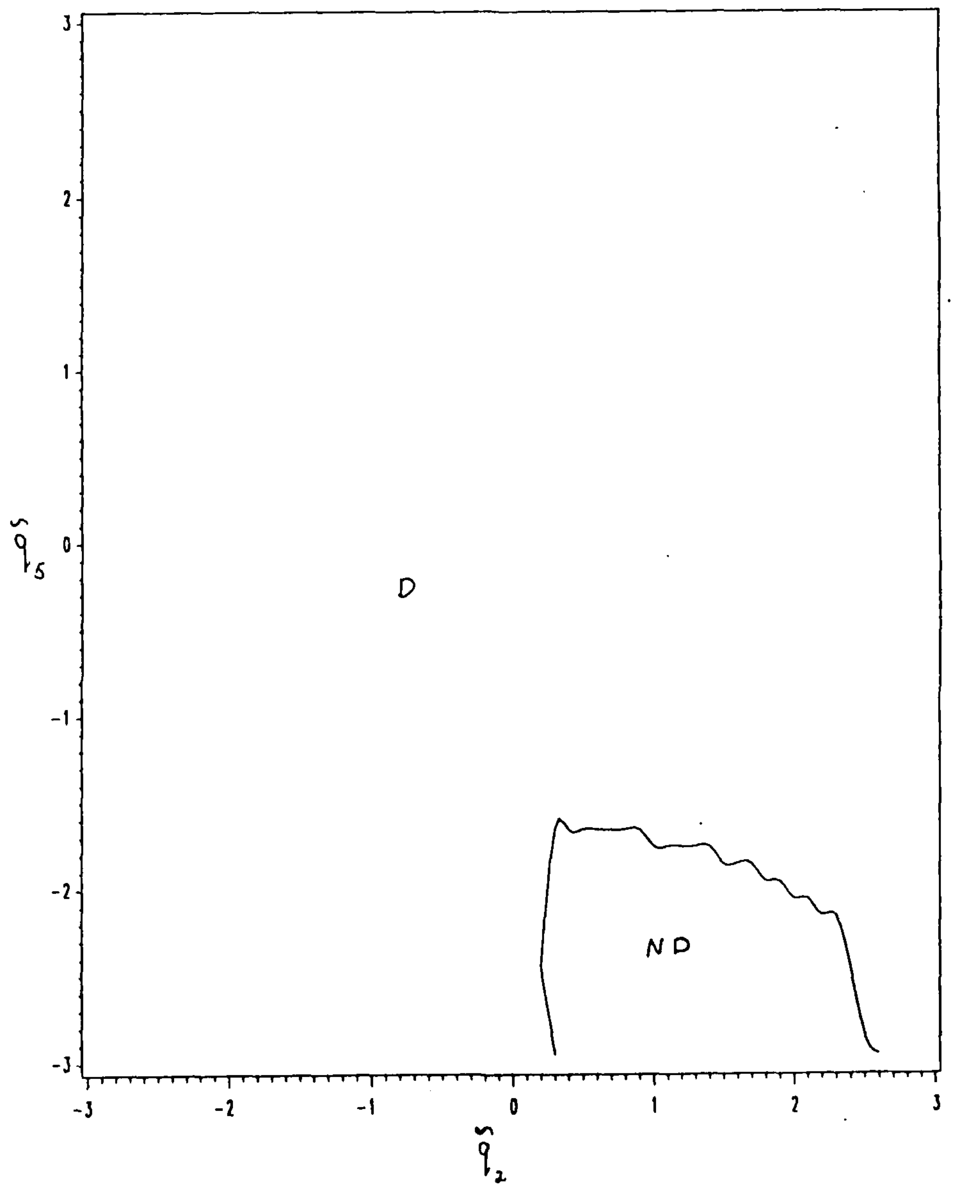

Figure 21: Regions of benchmark distinguishability of $F(q)$ from $F(p)$ for simultaneous measurement of the 2nd and 8th state variables.

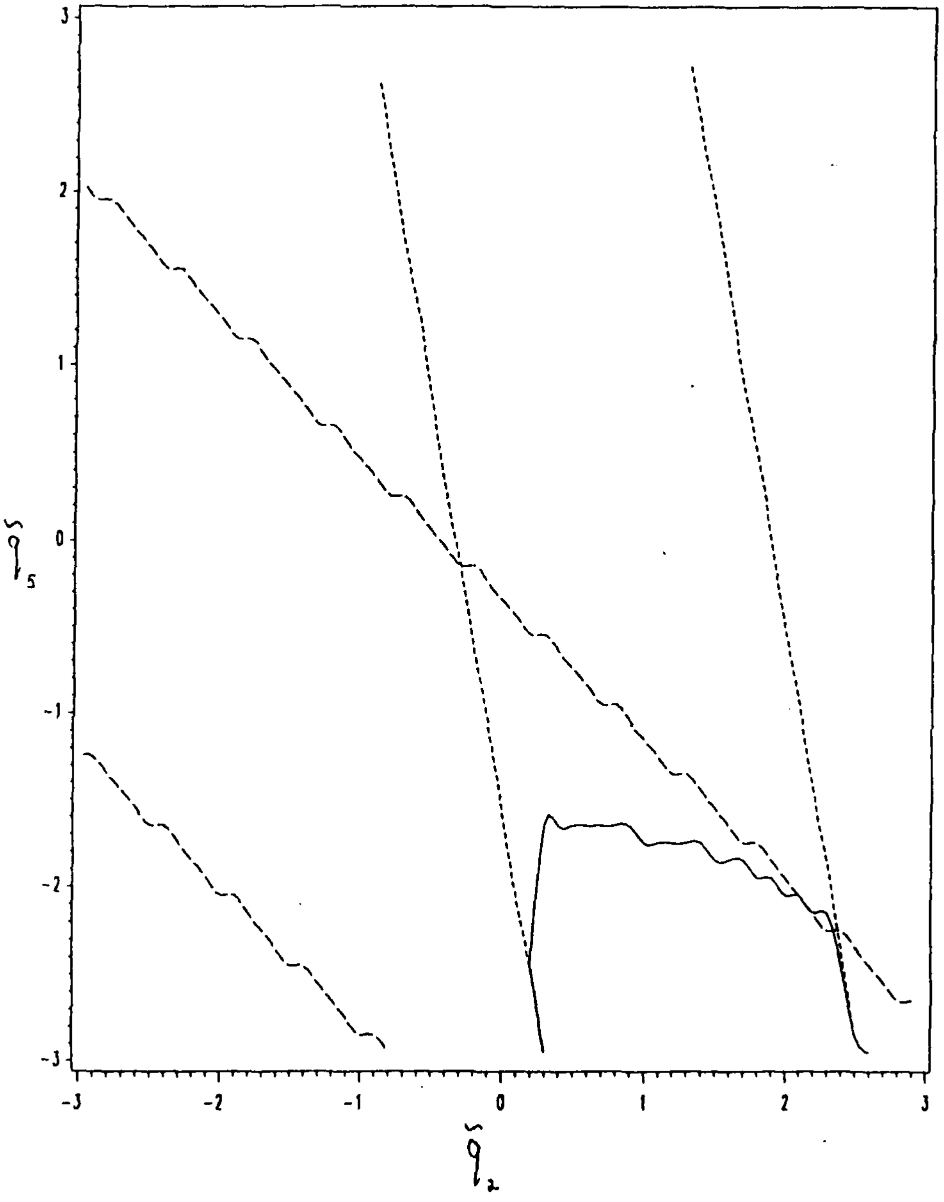

Figure 22: Regions of benchmark distinguishability of $F(q)$ from $F(p)$ for simultaneous measurement of the 2nd and 8th state variables (solid), and for single measurement of the 2nd (small dash) and the 8th (large dash) state variable.

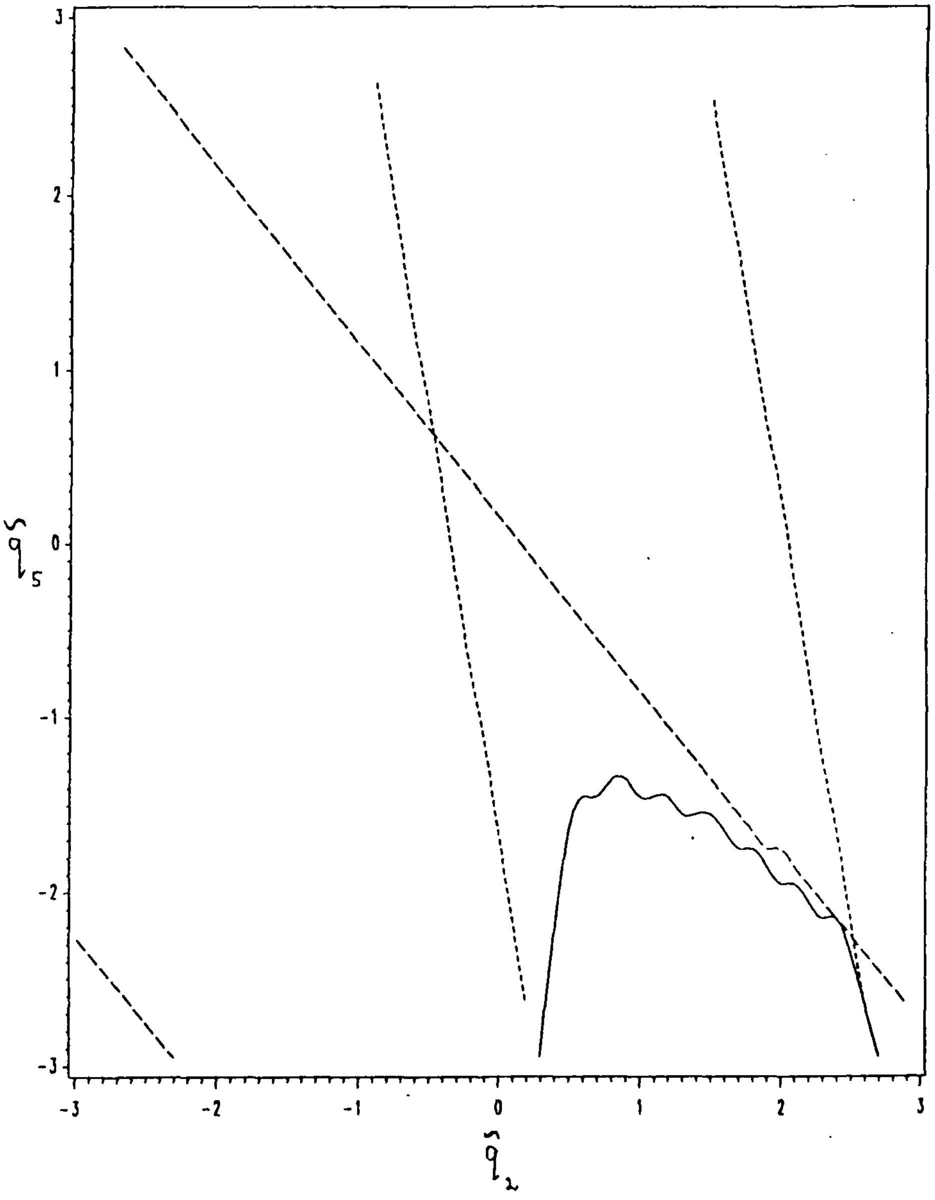

Figure 23: Regions of benchmark distinguishability of $F(q)$ from $F(p)$ for simultaneous measurement of the 1st and 6th state variables (solid), and for single measurement of the 1st (small dash) and the 6th (large dash) state variable.

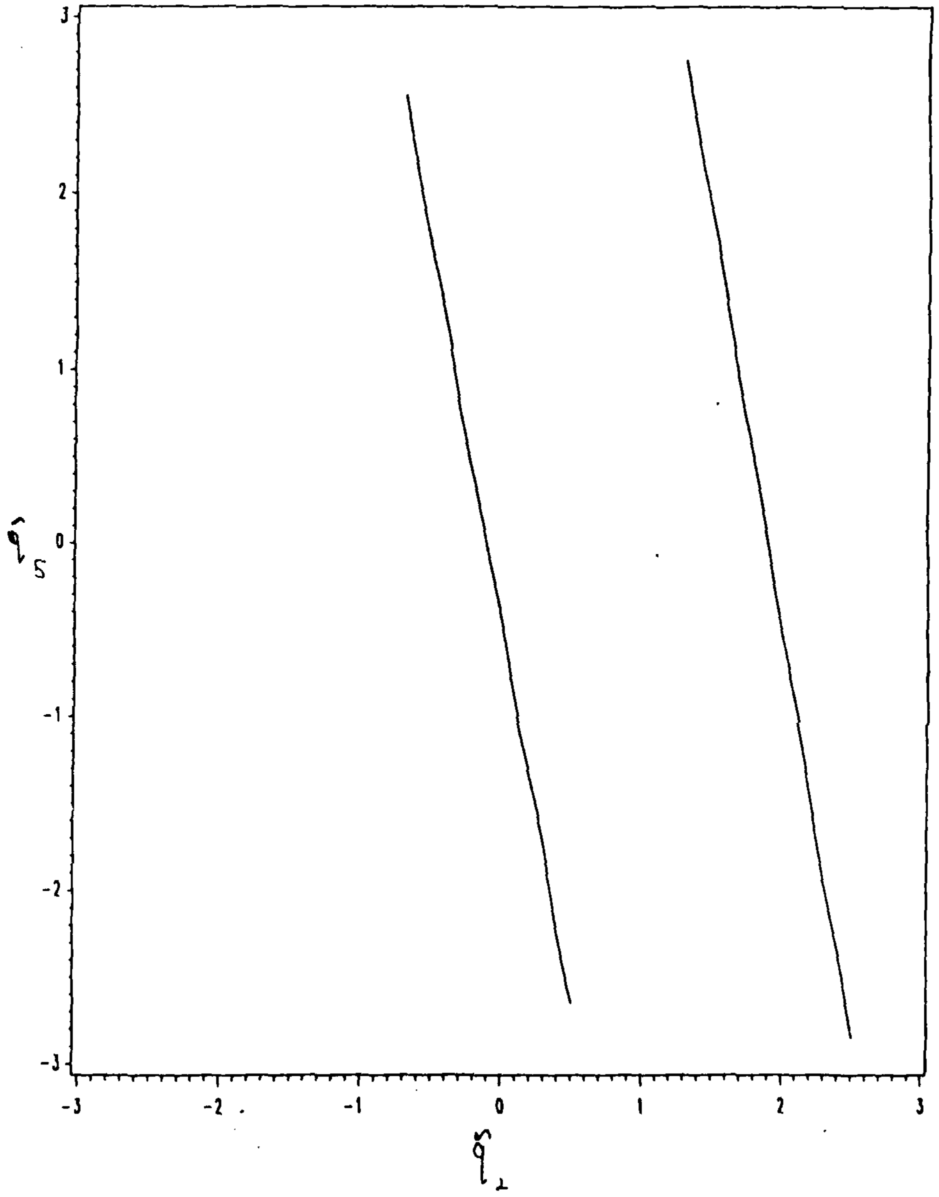

Figure 24: Regions of benchmark distinguishability of $F(q)$ from $F(p)$ for simultaneous measurement of the 2nd and 7th state variables.

Consider malfunction of J actuators, whose indices are $\mathbf{j} = (j_1, \ldots, j_J)$. Let $f(t)$ be an M-element vector whose j_kth element represents the autonomous behavior of the failed j_kth actuator, for $k = 1, \ldots, J$, and whose other elements are zero. Let E be a postive number and $\bar{f}(t)$ a specified vector function whose elements, other than the element $j_1, \ldots, j_J$, are zero. The set of possible control actuator failures is:

$$F(\bar{f}, E) = \left\{ f : \int_0^t \left(f(\tau) - \bar{f}(\tau)\right)^T \left(f(\tau) - \bar{f}(\tau)\right) d\tau \leq E \right\} \tag{29}$$

The elements of $F(\bar{f}, E)$ are vector functions whose elements $f_{j_1}, \ldots, f_{j_J}$ deviate from $\bar{f}(t)$ with an energy not exceeding E. (It is implicitly understood in the definition of $F(\bar{f}, E)$ that the $M - J$ other elements of f are identically zero).

Let $F(\bar{f}, E_1)$ be a set of energy-bounded failures in actuators $\mathbf{j} = (j_1, \ldots, j_J)$, and let $F(\bar{g}, E_2)$ be a set of energy-bounded failures in actuators $\mathbf{k} = (k_1, \ldots, k_J)$. Let $X_{\mathbf{j}}(t)$ and $X_{\mathbf{k}}(t)$ be the corresponding transition matrices.

From the discussion in section 6.1 it is evident that every failure in $F(\bar{f}, E_1)$ can be distinguished from every failure in $F(\bar{g}, E_2)$, and thus these failure sets are benchmark distinguishable, if and only if there exists a vector ω such that:

$$\max_{f \in F(\bar{f}, E_1)} \omega^T y_f < \min_{g \in F(\bar{g}, E_2)} \omega^T y_g \tag{30}$$

We now proceed to develop explicit expressions for these extrema. Let $y_{\mathbf{j}}^o(t)$ and $y_{\mathbf{k}}^o(t)$ be defined as before and define:

$$\Psi_{\mathbf{j}}(t, \tau) = G(t) X_{\mathbf{j}}(t) X_{\mathbf{j}}^{-1}(\tau) B(\tau) \tag{31}$$

$$\Psi_{\mathbf{k}}(t, \tau) = G(t) X_{\mathbf{k}}(t) X_{\mathbf{k}}^{-1}(\tau) B(\tau) \tag{32}$$

Then, for $f \in F(\bar{f}, E_1)$,

$$\omega^T y_f(t) = \omega^T y_{\mathbf{j}}^o(t) + \int_0^t \omega^T \Psi_{\mathbf{j}}(t, \tau) f(\tau)\, d\tau \tag{33}$$

$$\begin{aligned} &= \omega^T y^o_{\mathbf{j}}(t) + \int_0^t \omega^T \Psi_{\mathbf{j}}(t,\tau)\left(f(\tau) - \bar{f}(\tau)\right) d\tau \\ &+ \int_0^t \omega^T \Psi_{\mathbf{j}}(t,\tau)\bar{f}(\tau)\, d\tau \end{aligned} \tag{34}$$

Likewise, for $g \in F(\bar{g}, E_2)$,

$$\begin{aligned} \omega^T y_g(t) &= \omega^T y^o_{\mathbf{k}}(t) + \int_0^t \omega^T \Psi_{\mathbf{k}}(t,\tau)\left(g(\tau) - \bar{g}(\tau)\right) d\tau \\ &+ \int_0^t \omega^T \Psi_{\mathbf{k}}(t,\tau)\bar{g}(\tau)\, d\tau \end{aligned} \tag{35}$$

Let $u(t)$ and $v(t)$ be vector functions. The Cauchy inequality asserts that:

$$(u^T v)^2 \leq (u^T u)(v^T v) \tag{36}$$

with equality if u is proportional to v (Hardy, Littlewood and Pólya, 1952). The Schwarz inequality asserts that:

$$\left(\int \sqrt{u^T u}\sqrt{v^T v}\, dt\right)^2 \leq \int u^T u\, dt \int v^T v\, dt \tag{37}$$

with equality if $\sqrt{u^T u}$ is proportional to $\sqrt{v^T v}$. Thus,

$$\int u^T v\, dt \leq \sqrt{\int u^T u\, dt \int v^T v\, dt} \tag{38}$$

with equality if u is proportional to v. By a similar argument one finds that

$$\int u^T v\, dt \geq -\sqrt{\int u^T u\, dt \int v^T v\, dt} \tag{39}$$

again with equality if u is proportional to v.

We now apply relation (38) to eq.(34) to find the maximum of $w^T y_f$. The function f can be chosen from $F(\bar{f}, E_1)$ so that $f - \bar{f}$ is proportional to $\Psi_{\mathbf{j}}^T \omega$. Because f belongs to $F(\bar{f}, E_1)$ the energy of deviation of f from $\bar{f}$ equals E_1.

Employing these considerations and relation (38) one finds the maximum of the expression in eq.(34) to be:

$$\begin{aligned}\max_{f\in F(\bar{f},E_1)} \omega^T y_f(t) &= \omega^T y_{\mathbf{j}}^o(t) + \int_0^t \omega^T \Psi_{\mathbf{j}}(t,\tau)\bar{f}(\tau)\,d\tau \\ &+ \sqrt{E_1}\sqrt{\int_0^t \omega^T \Psi_{\mathbf{j}}(t,\tau)\Psi_{\mathbf{j}}^T(t,\tau)\omega d\tau} \qquad (40)\end{aligned}$$

By a similar argument one finds that the minimum of $\omega^T y_g$ is:

$$\begin{aligned}\min_{g\in F(\bar{g},E_2)} \omega^T y_g(t) &= \omega^T y_{\mathbf{k}}^o(t) + \int_0^t \omega^T \Psi_{\mathbf{k}}(t,\tau)\bar{g}(\tau)\,d\tau \\ &- \sqrt{E_2}\sqrt{\int_0^t \omega^T \Psi_{\mathbf{k}}(t,\tau)\Psi_{\mathbf{k}}^T(t,\tau)\omega d\tau} \qquad (41)\end{aligned}$$

Now eqs.(40) and (41) can be combined with relation (30) to obtain an expression for the necessary and sufficient condition for the benchmark distinguishability of $F(\bar{f}, E_1)$ from $F(\bar{g}, E_2)$.

6.5 Benchmark Diagnosis: Conclusions

Two types of failures - each represented by a failure set — are benchmark distinguishable if the corresponding response sets are disjoint. Benchmark distinguishability means that it is possible, in principle, to distinguish between these two failure types in all their possible manifestations. On the other hand, no algorithm can distinguish between every possible manifestation of failures belonging to failure sets which are benchmark indistinguishable. This report has developed a method for evaluating benchmark distinguishability for control actuator failures. The following conclusions and implications can be identified.

1. The benchmark distinguishability of a system assesses the malfunction diagnostic capability inherent in the system. It does so by exploiting fragmentary information about the range of possible failures. This is important since detailed

knowledge about failure systematics — such as required in formulating a probabilistic model of malfunction — is rarely available.

2. Benchmark distinguishability is a conservative assessment of the malfunction diagnostic properties of a system, in the following sense. Two failure sets are benchmark indistinguishable even if "most" but not all of the (infinity) of failures in each set are distinguishable. On the other hand, this conservatism can be balanced by evaluating the benchmark distinguishability of failure sets whose complete distinguishability is essential for successful malfunction management.

3. Malfunction diagnosis is often formulated as a multi-hypothesis decision problem. In the multi-hypothesis approach the observed behavior of the system is compared against the behavior expected from each of a finite set of postulated, archetypical failures. The performance of a multi-hypothesis algorithm for malfunction diagnosis is limited by the disparity between its finite set of hypothesized malfunctions and the infinity of possible failures. In section 7 we develop a method for evaluating the ability of a multi-hypothesis algorithm to distinguish between convex failure sets. Viewed from the perspective of multi-hypothesis diagnosis, the benchmark diagnosis capability of a system is seen to express the malfunction diagnosis performance which would be obtained with a judiciously chosen and *infinite* selection of failure hypotheses (in the absence of noise). As such, the benchmark capability provides a limiting measure of performance against which the diagnostic capabilities of a finite algorithm can be compared.

4. It is important to stress that, while the benchmark distinguishability can be viewed as the performance of an infinite dimensional multi-hypothesis algorithm, the benchmark distinguishability is not evaluated numerically as the limit of a sequence of finite designs. This would be impractical. Rather, the benchmark distinguishability is evaluated very simply for additive failures in linear systems by exploiting the convexity of the failure and response sets. The geometric concept of hyperplane separation leads directly to a sequence of linear optimization problems whose result is the determination of the benchmark diagnosis capability.

5. Application of the concept of benchmark distinguishability to the diagnosis of control actuator failures in linear flight of an AFTI/F16 aircraft leads to the conclusion that measurement of even a single state variable can provide substantial malfunction diagnostic capability. Furthermore, the benchmark analysis of the single-measurement diagnosis led to the identification of double measurements whose diagnostic capability is fairly comprehensive.

6. Finally, it must be stressed that the concept of benchmark distinguishability is not, in itself, a method for malfunction diagnosis. Rather, benchmark distinguishability provides a measure of the malfunction diagnosis capability which is inherent in the system being controlled. As such, benchmark distinguishability can serve as an objective quantitative aid in the design of a malfunction diagnosis algorithm.

7 Multi-Hypothesis Malfunction Distinguishability

7.1 Formulation of Multi-Hypothesis Diagnosis

In[2] this subsection we state the maximum-likelihood multi-hypothesis approach to diagnosing additive failures in linear dynamic systems and formulate the problem to be studied. Let $f(t)$ be a vector function representing a specific control-actuator malfuntion, and let $y_f(t)$ represent the average measured system response to $f(t)$. Because the system is linear and the failure is additive, $y_f(t)$ is an affine transformation of $f(t)$. (The specific form which $y_f(t)$ assumes for control actuator failure will be discussed later.) Throughout the report we let E^L represent a Euclidean space of dimension L to which measurement vectors y belong. Let $p(y|f)$ be the conditional probability density of the system response given a malfunction f. We shall assume that $p(y|f)$ decreases monotonically with a norm of $y - y_f$. This re-

[2] The results of section 7 will appear in the AIAA *Journal of Guidance, Control and Dynamics*, Ben-Haim (1989b).

quirement is fulfilled, for example, if $p(y|f)$ is a multivariate Gaussian density and if the square of the norm of y is $y^T V_f^{-1} y$, where V_f is the covariance matrix of y given malfunction f. The superscript T implies matrix transposition. Different norms can be defined with respect to different malfunctions, for example if the covariance matrix depends on the malfunction. We denote the various norms as follows. An inner product of elements x and y in E^L, with respect to the malfunction f, is denoted $[x,y]_f$. Our only assumption regarding this inner product is that $[x,y]_f^{1/2}$ is a norm, which will be denoted $\| x \|_f$.

Many distinct classes of actuator failures can occur: single or multiple failures; locked surfaces or widely varying surface deflections. In an important class of malfunctions the affected control surfaces fail to trail the control commands. Instead, these control surfaces deflect autonomously. The failure vectors $f(t)$ are assumed to belong to a set of uniformly bounded but otherwise freely varying functions. The failure sets are defined in section 5 as:

$$F(p) = \{f^T = (f_1, \ldots, f_M) : \ \tilde{p}_m \le f_m(t) \le \hat{p}_m \ \ , \ \ t \in [0, \infty) \ \ , \ \ m = 1, \ldots, M\} \tag{42}$$

where $p = (\tilde{p}_1, \hat{p}_1, \ldots, \tilde{p}_M, \hat{p}_M)$. Thus the autonomous value of the mth control function varies arbitrarily in time between $\tilde{p}_m$ and $\hat{p}_m$. Usually the number of actuator failures is less than the dimension of the control vector. This is represented by choosing $\tilde{p}_m = \hat{p}_m = 0$ for each of the functioning actuators. $F(p)$ will be referred to as the ***failure set*** for malfunctions of type p. The set $F(p)$ is convex.

Let $F(p^1), \ldots, F(p^K)$ be disjoint failure sets and let H_k be a finite collection of malfunctions chosen from $F(p^k)$, for $k = 1, \ldots, K$. Let $H = \cup_{k=1}^{K} H_k$. A maximum-likelihood multi-hypothesis algorithm for malfunction diagnosis is based on the collection H of vector functions representing hypothesized malfunctions. Having obtained a measurement, y, the algorithm seeks a hypothesized malfunction $h_{ml} \in H$ which satisfies:

$$\| y_{h_{ml}} - y \|_{h_{ml}}^2 = \min_{h \in H} \| y_h - y \|_h^2 \tag{43}$$

The function h_{ml} is most likely to be the system condition which caused the measurement y, because $p(y|h)$ decreases monotonically with $\| y - y_h \|_h$.

Given failure sets $F(p^1), \ldots, F(p^K)$ and given sets of hypothesized malfunctions $H_1, \ldots, H_K$, we will say that failures of type p^k are ***correctly diagnosed*** if every failure in $F(p^k)$ is ascribed by the multi-hypothesis algorithm to a hypothesized failure in H_k. A collection $H = \cup_{k=1}^{K} H_k$ of malfunction hypotheses is ***robust*** if the failure sets $F(p^1), \ldots, F(p^K)$ are correctly diagnosed. A robust collection H of malfunction hypotheses is ***efficient*** if no smaller set of hypotheses is robust. The problem to be studied here is to develop a computationally feasible method for determining whether or not a given set of hypothesized malfunctions is robust. This determination forms the basis for searching for an efficient collection of hypotheses.

An important simplification occurs when the norms $\| \cdot \|_{h_k}$ are the same for all hypothesized malfunctions. An example is developed in section 7.3 for actuator failures in an open-loop linear system.

7.2 Representing Uniformly Bounded Control-Actuator Failures

Our aim in this section is to develop a convenient formalism for representing the measurements of a closed-loop linear system with uniformly bounded control-actuator failure. The main result of this section is eq.(55), which is an expression for the complete response set. Several relations from section 4 have been repeated for convenience.

Consider the failure-free dynamic system:

$$\frac{dx}{dt} = Ax(t) + Bu(t) + v_1(t) \tag{44}$$

$$y(t) = Gx(t) + v_2(t) \tag{45}$$

$$u(t) = S(t)x(t) \tag{46}$$

where x, y, and u are state, measurement and control vectors of dimension N, L and M, respectively, v_1 and v_2 are zero-mean white Gaussian noise vectors with known, constant covariance matrices, and A, B and G are known constant matrices. The choice of the feedback gain matrix $S(t)$ is immaterial to our discussion.

Let us now consider the representation of J control actuator failures. The indices of the failed actuators are $\mathbf{j} = (j_1, \ldots, j_J)$. When a malfunction occurs in the j_kth control actuator its normal control function, $u_{j_k}(t)$, is replaced by an autonomous expression, $f_{j_k}(t)$. Let $f(t)$ be an M-element vector whose j_kth element is the autonomous behaviour of the failed j_kth actuator, for $k = 1, \ldots, J$, and whose other elements are zero. Let $I_{\mathbf{j}}$ be the matrix obtained from the $M \times M$ identity matrix by removing each of the J rows $j_1, \ldots, j_J$. Thus $I_{\mathbf{j}}u(t)$ is a vector obtained by removing the elements $j_1, \ldots, j_J$ from the nominal control vector, $u(t)$. Similarly, $BI_{\mathbf{j}}^T$ is an $N \times (M - J)$ matrix obtained by removing the columns $j_1, \ldots, j_J$ from the matrix B. Using this notation, the dynamic response of the system to failure of J actuators whose indices are $\mathbf{j}$ is described by:

$$\frac{dx}{dt} = Ax(t) + BI_{\mathbf{j}}^T I_{\mathbf{j}}u(t) + Bf(t) + v_1(t) \qquad (47)$$

The normal control algorithm still calculates the feedback control vector from eq.(46). However, $f_{j_k}(t)$ is implemented rather than $u_{j_k}(t)$. Combining eqs.(46) and (47) yields:

$$\frac{dx}{dt} = \left[A + BI_{\mathbf{j}}^T I_{\mathbf{j}}S(t)\right] x(t) + Bf(t) + v_1(t) \qquad (48)$$

The state vector $x(t)$ can be expressed in terms of a transition matrix $X_{\mathbf{j}}(t)$, which is the solution of the following differential equation [14]:

$$\frac{dX_{\mathbf{j}}}{dt} = \left[A + BI_{\mathbf{j}}^T I_{\mathbf{j}}S(t)\right] X_{\mathbf{j}}(t) \quad , \quad X_{\mathbf{j}}(0) = I \qquad (49)$$

Finally, the measurement vector (with noise) in response to failure vector $f(t)$ is:

$$\tilde{y}_f(t) = GX_{\mathbf{j}}(t)x(0) + G\int_0^t X_{\mathbf{j}}(t)X_{\mathbf{j}}^{-1}(\tau)(Bf(\tau) + v_1(\tau))\,d\tau + v_2(t) \qquad (50)$$

Unless $S(t) = 0$ (the open-loop case) the transition matrix, $X_{\mathbf{j}}$, depends on which actuators are malfunctioning, so the covariance matrix of $\tilde{y}_f$ depends on the failure. Consequently the quadratic norm, based on the covariance matrix of the measurement, varies with the failure.

The failure set for malfunctions of type p is $F(p)$, as in eq.(42). Each failure $f(t)$ in $F(p)$ is mapped to an average measurement vector $y_f(t)$ (without noise) in measurement space (eq.(50) with $v_1 = v_2 = 0$). Let $C(p)$ be the set of all the average measurement vectors obtained from failures in the set $F(p)$. That is:

$$C(p) = \{y : \; y(t) = y_f(t) \quad \text{for all} \quad f \in F(p)\} \tag{51}$$

We will call $C(p)$ the *complete response set* for failures of type p. Since the failure set $F(p)$ is convex, the response set $C(p)$ is likewise convex because $y_f(t)$ is an affine transformation of f.

It is more convenient, however, to define $C(p)$ in terms of its boundary. Define the constant failure vector $\bar{p} = (\bar{p}_1, \ldots, \bar{p}_M)$, where $\bar{p}_m = (\hat{p}_m + \tilde{p}_m)/2$ for $m = 1, \ldots, M$. Let $y(t)$ be the average response to the constant failure $\bar{p}$, so $\bar{y}(t) = y_{\bar{p}}(t)$. That is,

$$\bar{y}(t) = G X_{\mathbf{j}}(t) x(0) + G \int_0^t X_{\mathbf{j}}(t) X_{\mathbf{j}}^{-1}(\tau) B \bar{p} \, d\tau \tag{52}$$

Let $F^*(p)$ be the set:

$$F^*(p) = \left\{ f^T = (f_1, \ldots, f_M) : \; |f_m(t)| \le \frac{\hat{p}_m - \tilde{p}_m}{2} \right\} \tag{53}$$

Every element g in $F(p)$ can be expressed as $g = \bar{p} + f$ where f belongs to $F^*(p)$. Thus the response to g can be expressed as the sum of the response to $\bar{p}$ and the response to f. Let $\Psi(t, \tau) = G X_{\mathbf{j}}(t) X_{\mathbf{j}}^{-1}(\tau) B$. Now the response set $C(p)$ can be expressed as:

$$C(p) = \left\{ y : \; y = y(t) + \int_0^t \Psi(t, \tau) f(\tau) \, d\tau \quad \text{for} \quad f \in F^*(p) \right\} \tag{54}$$

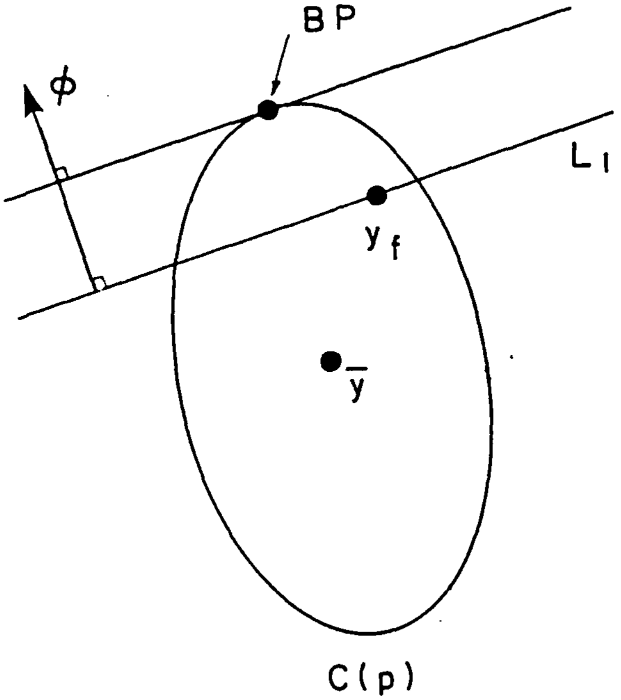

Figure 25: Illustration of the procedure for finding boundary points of $C(p)$.

From this expression it is evident that $C(p)$ is convex, contains the point $\bar{y}(t)$ and is symmetric with respect to inversion through $\bar{y}(t)$. Also, every element of $C(p)$ can be expressed as $y = \bar{y}(t) + \alpha\rho(\omega)\omega$ where ω is a unit vector in the direction from $\bar{y}$ to y, $\rho(\omega)$ is the distance along ω from $\bar{y}$ to the boundary of $C(p)$ and $0 \leq \alpha \leq 1$. That is, the complete response set can be represented as:

$$C(p) = \left\{ y : \ y = \bar{y}(t) + \alpha\rho(\omega)\omega \ \ , \ \ 0 \leq \alpha \leq 1, \ \ \omega^T\omega = 1 \right\} \tag{55}$$

To evaluate the radius function $\rho(\omega)$ we must first identify the elements of F^* which generate the boundary points of $C(p)$. Let ϕ be a vector in E^L. For a given

$f \in F^*(p)$, the set of points z which satisfy:

$$\phi^T z = \phi^T \left(\bar{y}(t) + \int_0^t \Psi(t,\tau) f(\tau)\, d\tau \right) \tag{56}$$

constitutes a plane in E^L through the point y_f and perpendicular to ϕ, as shown by the line L_1 in Figure 25. The distance of this plane from $\bar{y}$ is:

$$\mathrm{dis}(y_f, \bar{y}) = \frac{1}{\sqrt{\phi^T \phi}} \left| \phi^T \int_0^t \Psi(t,\tau) f(\tau)\, d\tau \right| \tag{57}$$

This distance varies as f varies on the set F^*. That element of F^* which maximizes $\mathrm{dis}(y_f, \bar{y})$ defines a boundary point of $C(p)$, denoted **BP** in Figure 25. Let $\psi^m(t,\tau)$ represent the mth column of $\Psi(t,\tau)$. Then $\mathrm{dis}(y_f, \bar{y})$ is maximized on F^* when the elements of the vector f are chosen as[3]

$$f_m(\tau;\phi) = \frac{\hat{p}_m - \tilde{p}_m}{2} \mathrm{sgn}(\phi^T \psi^m(t,\tau)) \quad , \quad m = 1, \ldots, M \tag{58}$$

where $\mathrm{sgn}(x) = \pm 1$, matching the sign of x. Boundary points of $C(p)$ are now represented as:

$$y(t;\phi) = \bar{y}(t) + \int_0^t \Psi(t,\tau) f(\tau;\phi)\, d\tau \tag{59}$$

where $f(\tau;\phi)$ in this expression is defined in eq.(58). Distinct boundary points are obtained by varying ϕ. Each boundary point in turn defines a value of the radius vector. For each ϕ the radius of $C(p)$ along direction $\omega = y(t;\phi) - \bar{y}(t)$ is $\sqrt{\omega^T \omega}$, which can be tabulated numerically as a function of the direction ω. Let $\rho(\omega)$ represent this tabulation. The argument of ρ need not be a normalized vector, but we will adopt the convention that, for any scalar $\alpha, \rho(\alpha\omega) = |\alpha| \rho(\omega)$ and that $\rho(\omega)$ precisely equals the radius of $C(p)$ along ω when ω is a unit vector.

[3] A similar maximization problem is discussed in eqs.(64)–(68), to which the reader is referred for justification of eq.(58).

7.3 Designing the Multi-Hypothesis Diagnosis of Open-Loop Malfunctions

In the absence of feedback in the control loop ($S(t) = 0$ in eq.(46) and $u(t)$ is independent of x) the transition matrix, eq.(49), is independent of the malfunction. Consequently the quadratic norm based on the covariance matrix of the measurement does not depend on the failure. Determination of the robustness of a collection H of hypothesized malfunctions can be based on the solution of a sequence of linear optimization problems, as shown in this section.

As in section 7.1, let $H = \cup_{k=1}^{K} H_k$ be the complete set of hypothesized malfunctions. Let g and h belong to H, and define the ***minimum relative norm*** on $C(p^k)$ with respect to g and h as:

$$D_k(g,h) = \min_{y \in C(p^k)} (\| y_g - y \|^2 - \| y_h - y \|^2) \tag{60}$$

If $D_k(g,h)$ is positive, then every occurrence of failure of type p^k will be ascribed to hypothesized malfunction h rather than to g. It is evident from the definition of correct diagnosis that failures of type p^k are correctly diagnosed if, for each $g \in H - H_k$, there is an element $h \in H_k$ such that

$$D_k(g,h) \geq 0 \tag{61}$$

This means that, for every failure in $F(p^k)$, no hypothesis outside H_k will be chosen by the multi-hypothesis algorithm. Consequently type p^k failures will be correctly diagnosed.

Expanding the norms in eq.(60) in terms of the inner product, one finds:

$$D_k(g,h) = \| y_g \|^2 - \| y_h \|^2 - 2 \max_{y \in C(p^k)} [y_g - y_h, y] \tag{62}$$

The maximum on the righthand side does in fact exist since $[y_g - y_h, y]$ is a linear (and thus continuous) function from the compact set $C(p^k)$ to the real numbers. Consequently, determination of the correct diagnosis of failure type p^k is based on evaluating the maximum of the linear function $[y_g - y_h, y]$ on $C(p^k)$, for each g and h in H. Eq.(43) indicates that the multi-hypothesis algorithm itself evaluates a quadratic expression in y. The adequacy of a linear expression for determining correct diagnosis derives from the fact, expressed in eq.(60), that correct diagnosis is established by comparing norms which are independent of the hypothesized malfunctions.

7.4 Example: Designing Multi-Hypothesis Diagnosis

To illustrate this analysis, we consider part of the design process for constructing a maximum-likelihood multi-hypothesis algorithm for diagnosing control actuator failures in AFTI/F16 aircraft in steady open-loop flight at 0.9 Mach and 20,000 feet altitude. The dynamic behavior and measurements of the failure-free linear system are represented by eqs.(44)-(46) with $S(t) = 0$. The 8 state variables, in order of their appearance in x, are: pitch angle, forward velocity, angle of attack, pitch rate, bank angle, sideslip angle, roll rate and yaw rate. The 6 control variables, in order of their appearance in u, are: right and left horizontal tails (elevators), right and left wing flaps, canards (operated symmetrically) and rudder. These control variables are zero in steady open-loop flight, but vary automatically after failure. G is the 8×8 identity matrix and the values of A and B are presented in tables (1) and (2).

We will now develop an explicit expression for the maximum in eq.(62). Let the initial state vector be $x(0) = 0$. From eqs.(44) and (45) one finds the average response to the malfunctioning control vector u to be:

$$y_u(t) = \int_0^t G e^{A(t-\tau)} B u(\tau)\, d\tau \qquad (63)$$

Let the inner product take the form $[x, y] = x^T V^{-1} y$, where V is the covariance matrix of the response vector. Also, let $\lambda^m(t, \tau)$ be the mth column of the matrix

$V^{-1}Ge^{A(t-\tau)}B$. Let $\delta(t) = y_g(t) - y_h(t)$. Then one finds:

$$[y_g(t) - y_h(t), y_u(t)] = \sum_{m=1}^{M} \int_0^t \delta(t)^T \lambda^m(t,\tau) u_m(\tau)\, d\tau \tag{64}$$

Examination of eq.(64) shows that the mth integral achieves its maximum when $u_m(\tau)$ is chosen to switch between its extremal values as $\delta(t)^T \lambda^m(t,\tau)$ changes sign. Specifically, eq.(64) is maximized by choosing the elements of u as:

$$\begin{aligned} u_m(\tau) &= \hat{p}_m \text{ for } \delta(t)^T \lambda^m(t,\tau) \geq 0 \qquad (65)\\ &= \tilde{p}_m \text{ for } \delta(t)^T \lambda^m(t,\tau) < 0 \qquad (66) \end{aligned}$$

Let D_{m+} and D_{m-} denote the subsets of the interval $[0,t]$ for which $\delta(t)^T \lambda^m(t,\tau)$ is non-negative and negative, respectively. Thus the maximum value of the inner product becomes:

$$\begin{aligned} \max_{u \in F(p^k)} [y_g(t) &- y_h(t), y_u(t)] \\ &= \sum_{m=1}^{M} \left\{ \hat{p}_m \int_{D_{m+}} \delta(t)^T \lambda^m(t,\tau)\, d\tau + \tilde{p}_m \int_{D_{m-}} \delta(t)^T \lambda^m(t,\tau)\, d\tau \right\} \qquad (67)\\ &= \sum_{m=1}^{M} \left\{ \frac{\hat{p}_m + \tilde{p}_m}{2} \int_0^t \delta(t)^T \lambda^m(t,\tau)\, d\tau + \frac{\hat{p}_m - \tilde{p}_m}{2} \int_0^t |\delta(t)^T \lambda^m(t,\tau)|\, d\tau \right\} \qquad (68) \end{aligned}$$

The minimum relative norm on $C(p^k)$ with respect to g and h is obtained by substituting eq.(68) in eq.(62). We are now able to determine whether or not a given collection of hypothesized malfunctions is robust.

The starting point for selecting hypothesized failures is specification of the failure sets which must be correctly diagnosed. Identification of a robust and efficient set of hypothesized malfunctions is then an iterative process. At least one hypothesis must be included in H for each failure set which is to be correctly diagnosed. Given an initial choice of H, eqs.(62) and (68) are used to determine whether or not the required failure sets are correctly diagnosed. Elements of H are

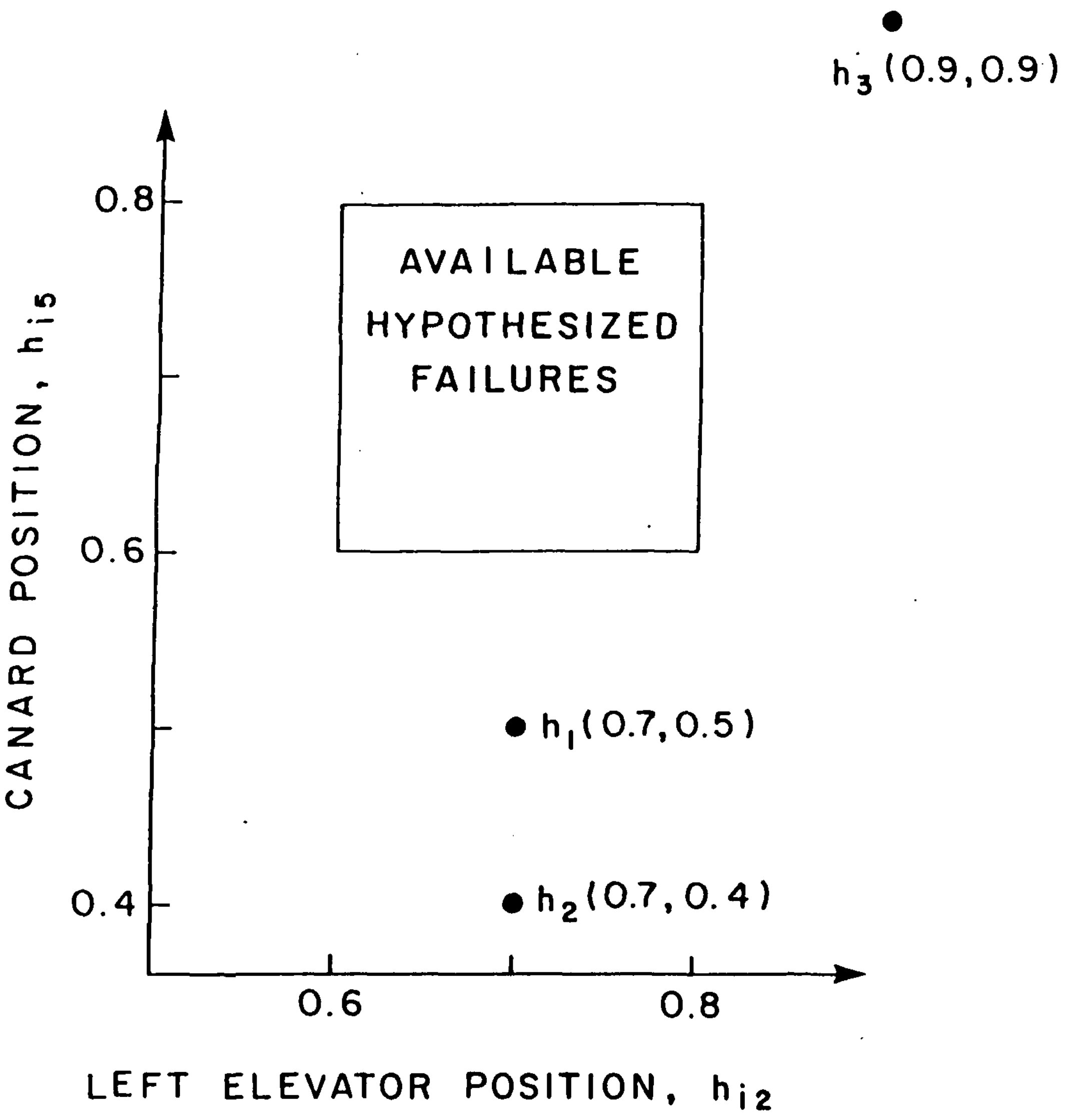

Figure 26: Hypothesized malfunctions represented by points in the h_{i2} versus h_{i5} plane.

then modified and new elements are included, until correct diagnosis is attained for each specified failure set.

The procedure for determining the robustness of a given set of hypotheses can be inverted, in part, to aid in the search for hypothesized malfunctions. A simple numerical example will illustrate this analysis. Suppose it is desired to correctly diagnose malfunctions of failures in the second and fifth control functions (left elevator and canards), when these control surfaces are deflecting autonomously. For graphical simplicity we will select hypothesized malfunctions h_i which are constant in time and non-zero only in the second and fifth elements. Thus hypothesized malfunctions can be represented as points in the plane, where the horizontal and vertical coordinates are the second and fifth elements of the failure vector, h_{i2} and h_{i5} respectively. Three hypothesized malfunctions, h_1, h_2 and h_3 have been included in H to diagnose other failures, as shown in Figure 26. It is now desired to select the minimum set of hypotheses needed to assure correct diagnosis of left elevator and canard deflections between, for example, 0.6^o and 0.8^o. Let us denote this failure set $F(0.6, 0.8)$.

Each point in the square region of Figure 26 represents a constant failure in $F(0.6, 0.8)$. However not each such point, if used as a hypothesized malfunction, would yield correct diagnosis of the malfunctions in $F(0.6, 0.8)$. Let h be a point in the square region of Figure 26, and consider the maximum likelihood comparison between h and h_1. Eqs.(62) and (68) are used to evaluate $D(h_1, h)$, the minimum relative norm on $C(0.6, 0.8)$ with respect to h_1 and h. The minimum relative norm for each point h below the curve in Figure 27 is found to be positive, indicating that these hypotheses yield correct diagnosis of the failures in question, when compared with hypothesis h_1. The minimum relative norm of all points above the curve in Figure 27 is negative, which means that hypothesized failures above the curve will not yield correct diagnosis. Figure 28 shows a similar analysis based on comparison with h_2. Again the minimum relative norm, $D(h_2, h)$, is positive for points below

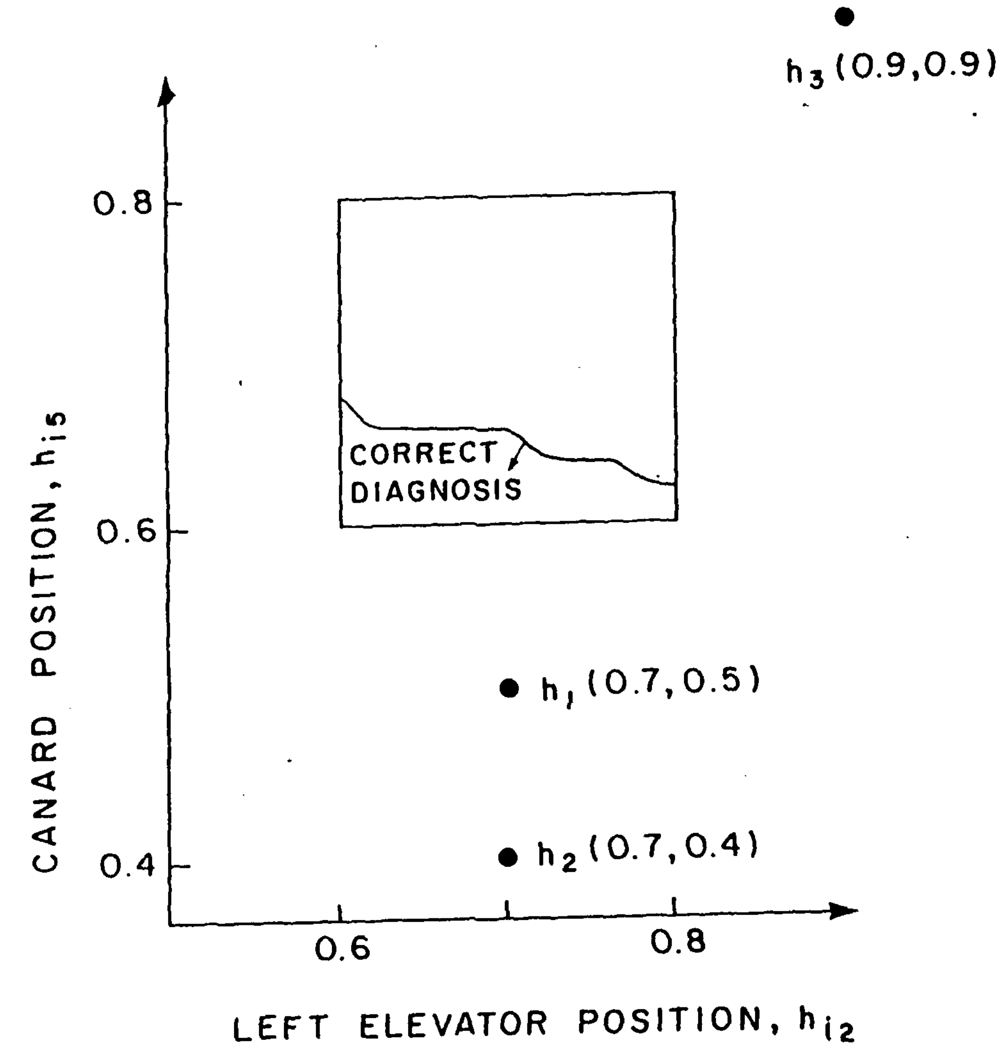

Figure 27: Malfunctions in the square region and below the curve yield correct diagnosis in comparison with h_1.

the curve and negative for points above the curve. Thus correct diagnosis in comparison with h_2 can be achieved only if a point below the curve in Figure 28 is included in H. Comparison of Figures 27 and 28 shows that correct diagnosis with respect to h_1 assures correct diagnosis with respect to h_2. The analysis is repeated to determine the hypothesized malfunctions which yield correct diagnosis in comparison with h_3, and the results appear in Figure 29. Points above the curve yield correct diagnosis of all failures in $F(0.6, 0.8)$, while points below the curve do not. Overlaying Figures 27 – 29 as in Figure 30, shows that two hypothesized malfunctions are necessary and sufficient to achieve correct diagnosis of all failures in $F(0.6, 0.8)$. One hypothesis must lie between the intermediate and upper curves, while one must lie below the lowest curve. Correct diagnosis of the failure set $F(0.6, 0.8)$ requires that two such hypotheses be included in H, as long as h_1, h_2 and h_3 are in H. Likewise, unless additional hypotheses are added to H for diagnosis of different failure sets, the two hypotheses which have been identified are sufficient to assure correct diagnosis of $F(0.6, 0.8)$. This analysis is continued until conditions are established for defining the smallest set of hypothesized malfunctions which assure correct diagnosis for each of the specified failure sets.

7.5 Designing The Multi-Hypothesis Diagnosis of Closed-Loop Malfunctions

Let $H = \cup_{k=1}^{K} H_k$, where each set H_k contains malfunctions drawn from the set $F(p^k)$ of uniformly bounded failures. The system is described by eqs.(44) and (45), and the feedback gain in eq.(46) is non-zero. We wish to determine whether or not malfunctions of type p^k are correctly diagnosed. Eq.(60) must be modified to account for the fact that, due to the feedback in the control loop, the quadratic norm depends on the failure. Accordingly, let g and h belong to H and define the minimum relative norm on $C(p^k)$ with respect to g and h as:

$$D_k(g, h) = \min_{y \in C(p^k)} \left(\| y_g - y \|_g^2 - \| y_h - y \|_h^2 \right) \qquad (69)$$

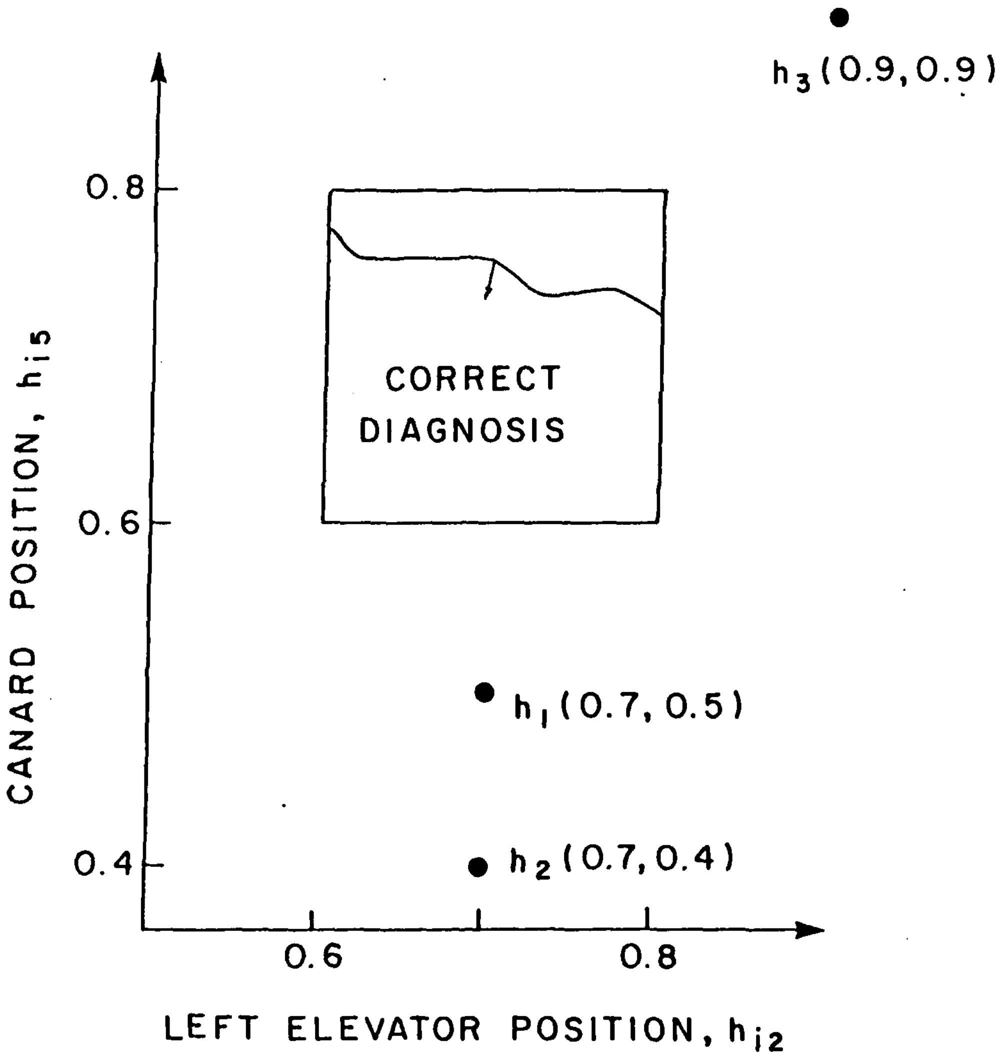

Figure 28: Malfunctions in the square region and below the curve yield correct diagnosis in comparison with h_2.

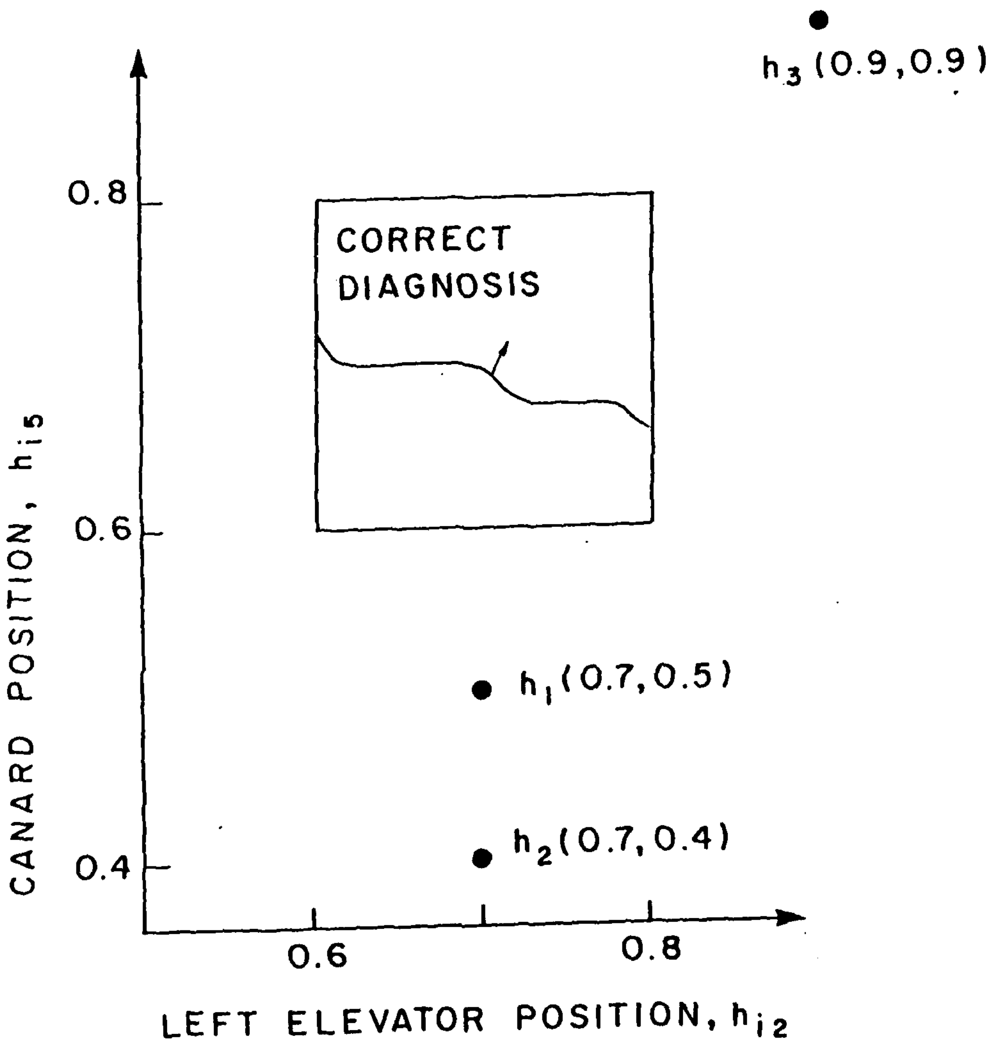

Figure 29: Malfunctions in the square region and above the curve yield correct diagnosis in comparison with h_3.

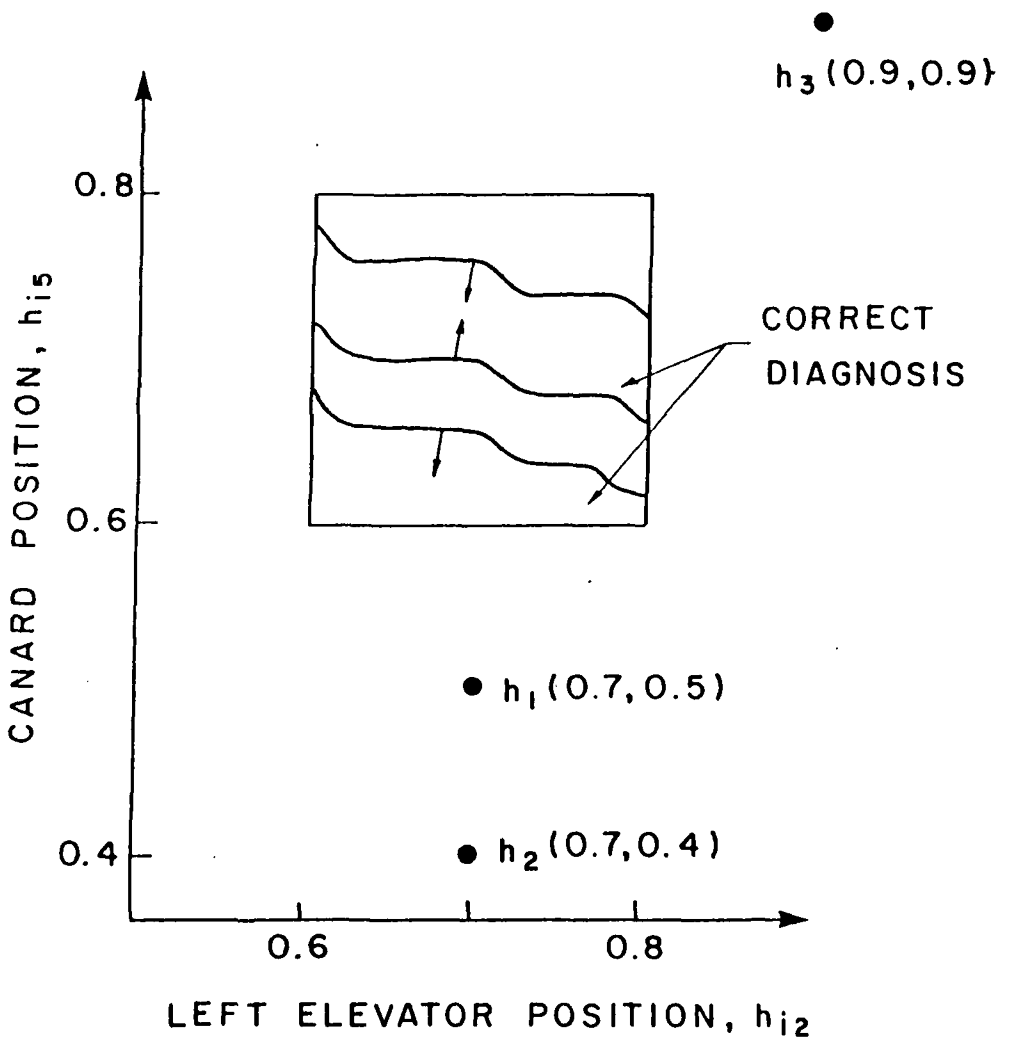

Figure 30: Overlay of the previous three figures, showing necessity of two hypothesized malfunctions for correct diagnosis in comparison with h_1, h_2 and h_3.

The main result of this section is the evaluation of this minimum relative norm. Once that is achieved, the hypothesized malfunctions are selected by the iterative procedure illustrated in section 7.4.

Let g and h be hypothesized malfunctions, and let y_g and y_h be the corresponding average responses. Let $y = \bar{y} + \eta$ be an element of $C(p^k)$, where $\bar{y}$ is defined, with respect to the parameters p^k, as in connection with eq.(54) and $\eta = \alpha\rho(\omega)\omega$ as in eq.(55). The expression to be minimized in eq.(69) becomes:

$$\begin{aligned} \| y_g - y \|_g^2 \;&-\; \| y_h - y \|_h^2 \\ &= (y_g - \bar{y} - \eta)^T V_g^{-1}(y_g - \bar{y} - \eta) - (y_h - \bar{y} - \eta)^T V_h^{-1}(y_h - \bar{y} - \eta) \qquad (70) \\ &= \eta^T \Delta \eta - 2\zeta^T \eta + \mu \qquad (71) \end{aligned}$$

where $\Delta = V_g^{-1} - V_h^{-1}$, $\zeta = V_g^{-1}(y_g - \bar{y}) - V_h^{-1}(y_h - \bar{y})$ and $\mu = \| y_g - \bar{y} \|_g^2 - \| y_h - \bar{y} \|_h^2$. Failures of type p^k are correctly diagnosed if, for each $g \in H - H_k$, there is an element $h \in H_k$ such that:

$$D_k(g, h) \geq 0 \qquad (72)$$

Referring to eq.(55) it is evident that η is a vector of arbitrary orientation whose length does not exceed the distance in direction η of $\bar{y}$ from the boundary of $C(p^k)$. Thus η is constrained by:

$$|\sqrt{\eta^T \eta}| \leq \rho\left(\frac{\eta}{\sqrt{\eta^T \eta}}\right) = \frac{1}{|\sqrt{\eta^T \eta}|}\rho(\eta) \qquad (73)$$

where $\rho(\omega)$ is determined numerically as explained in section 7.2. This inequality constraint on the maximization of eq.(71) can be replaced by an equality by introducing an undetermined quantity, β :

$$\eta^T \eta + \beta^2 = \rho(\eta) \qquad (74)$$

Adjoin the constraint to the expression in eq.(71) as:

$$D^* = \eta^T \Delta \eta - 2\zeta^T \eta + \mu + \lambda(\eta^T \eta + \beta^2 - \rho(\eta)) \qquad (75)$$

Necessary conditions for a stationary point of eq.(71) are:

$$0 = \frac{\partial D^*}{\partial \eta} = 2\Delta\eta - 2\zeta + 2\lambda\eta - \lambda\frac{\partial \rho}{\partial \eta} \tag{76}$$

$$0 = \frac{\partial D^*}{\partial \beta} = 2\lambda\beta \tag{77}$$

Eq.(77) together with the constraint imply that $\lambda = 0$ if $\eta^T\eta < \rho(\eta)$. Thus an extremum of eq.(71) occurs in the interior of $C(p^k)$ if the solution of:

$$\Delta\eta = \zeta \tag{78}$$

satisfies $\eta^T\eta < \rho(\eta)$. If not, then the extrema of eq.(71) occur on the boundary of $C(p^k)$ and must satisfy:

$$(\Delta + \lambda I)\eta = \zeta + \frac{1}{2}\lambda\frac{\partial \rho}{\partial \eta} \tag{79}$$

and

$$\eta^T\eta = \rho(\eta) \tag{80}$$

Eqs.(78) - (80) determine the constrained extrema of $D_k(g, h)$. Failures of type p^k are correctly diagnosed if the condition in eq.(72) is satisfied.

The solution of eqs.(79) and (80) is computationally somewhat cumbersome. It is therefore useful to know that, if Δ is a positive definite matrix, then eq.(71) has precisely one minimum and may have several local maxima. Or, if Δ is negative definite, then eq.(71) has precisely one maximum and may have several local minima. If Δ is indefinite, then eq.(71) can have several minima and maxima.

7.6 Multi-Hypothesis Diagnosis: Conclusions

This section has described a method for designing a maximum-likelihood multi-hypothesis algorithm for diagnosing control-actuator failures in linear systems. Uncertainty in the temporal behavior of a malfunctioning actuator is represented by employing the set theoretic technique called convex modelling. For open-loop systems (autonomous controllers) the diagnosis algorithm is designed by solving a sequence of linear optimization problems. For closed-loop feedback systems the design of the diagnosis algorithm requires the solution of non-linear equations. The resulting diagnosis algorithm is robust and efficient. Robust in that the diagnosis invariably distinguishes between failure sets which represent complex uncertainty in the temporal form of the malfunctions. Efficient in that no smaller set of hypothesized malfunctions could achieve correct diagnosis of the required classes of failures. The significance of this result is that design of an algorithm for diagnosis of control actuator failure can be based on a systematic and numerically implementable procedure which yields the best possible algorithm, in the sense of robustness and efficiency defined here.

8 Concluding Remarks and Future Research

The diagnosis of additive failures in a linear dynamic system has been studied in this project. This class of failures includes control-actuator failures, which are emphasized in this report. Several theoretical concepts relating to the design of control-actuator failure-diagnosis have been developed. Illustrative numerical examples have been presented based on a linearized steady-flight model of the AFTI/F16 aircraft.

The successful diagnosis of failure relies on knowledge of the malfunction phenomenon in general. However, malfunction is usually so complicated that it is unfeasible to formulate a probability measure which expresses the relative likelihood of each of the infinite range of possible specific malfunctions. On the other hand, sufficient partial information is often available with which to formulate a set-theoretic *convex model* of failure uncertainty. This approach has been adopted in the present study.

Convex modelling provides two distinct tools for optimization of malfunction diagnosis algorithms. The first, called ***benchmark diagnosis***, is an assessment of the best state space malfunction diagnosis capability which can be obtained by any algorithm, whether based on the multi-hypothesis maximum-likelihood concept or not. Evaluation of the optimum distinguishability is useful as a benchmark, against which the performance of implementable algorithms can be compared. Conclusions regarding benchmark diagnosis in general and its application to aircraft systems in particular have been discussed in section 6.5.

The second tool provided by convex modelling, called ***multi-hypothesis distinguishability,*** enables assessment of the malfunction diagnosis performance of a specific multi-hypothesis algorithm. This enables the quantitative comparison of the performance of multi-hypothesis malfunction diagnosis algorithms based on distinct sets of failure hypotheses. Optimization of the malfunction diagnosis algorithm is based on these comparisons. Implications of the results concerning multi-hypothesis diagnosis are discussed in section 7.6.

Several areas of further research are of immediate interest. Many engineering systems of importance in aeronautics and other fields display malfunctions which may be modelled as additive failures. The application of convex modelling to such systems can be pursued. This may include either different aerodynamic models than the one studied in this report, or different classes of failures. Alternatively, convex modelling can be applied to the development and optimization of algorithms for malfunction diagnosis in sub-systems, such as inertial navigation systems.

An additional problem area is the study of the algorithmic basis of convex modelling. The development of efficient computer algorithms for evaluating the disjointness of convex sets is essential for a large scale benchmark analysis. Rapid algorithms for evaluating the minimum relative norm are needed for optimizing the design of a multi-hypothesis diagnosis algorithm in a large complex system.

A further area of importance is the incorporation of the diagnosis task in the overall framework of malfunction management. Diagnosis of failure should lead to the implementation of a compensatory controller whose task is to lead to graceful recovery of the system. Central unsolved problems are:

1. Design the diagnosis algorithm to incorporate the subsequent needs of the compensatory controller.

2. Synthesize the compensatory controller.

3. Integrate the tasks of failure diagnosis and failure compensation so that management of the malfunction begins to be implemented before learning of the failure has been completed.

A final area of interest for further work is the study of non-additive failures. Important classes of malfunctions deviate from the assumption of additivity. In particular, those failures in which the model parameters (e.g. aerodynamic coefficients) undergo alteration violate the assumption of additivity. In such cases the property of convexity of the failure set is still plausible, and the general mode of thought of convex modelling is still relevant. However, difficulties develop which need to be studied both analytically and numerically.

Appendix
Plausibility of Convex Models of Uncertainty

In a set-theoretic model of malfunction uncertainty the malfunction is modelled as a time- or space-dependent vector function drawn from a set of possible functions. We wish to identify conditions in which it is plausible to assume such sets of functions are convex. The central limit theorem will motivate our discussion. Let $g_1, \ldots, g_n$ be independent, identically distributed random variables with zero mean and finite variance. As $n \to \infty$ the distribution of the sum $f = \frac{1}{\sqrt{n}}\Sigma g_i$ tends to a normal distribution, regardless of how the g_i are distributed. The physical analog of this theorem suggests that if a certain measurable macroscopic quantity f e.g. a voltage or a temperature is the superposition of numerous random, independent and identically distributed microscopic variables g_i, then we should expect the macroscopic quantity f to display a gaussian distribution, regardless of how the g_i are distributed. Indeed, this expectation is fulfilled in many circumstances.

Now let us consider a set-theoretic approach to modelling the uncertainty of a time-dependent macroscopic vector function f. Let Γ be a set of vector-valued functions. For a positive integer n, consider the set of functions:

$$F_n = \left\{ f : \ f(t) = \frac{1}{n}\sum_{i=1}^{n} g_i(t) \ , \ g_i \in \Gamma \ , \ i = 1, \ldots, n \right\} \tag{81}$$

It is well known (Aumann, 1965; Artstein, 1974; Artstein and Hansen, 1985) that, as $n \to \infty$, the sequence of sets F_n converges to the convex hull of Γ. This result invites the following physical interpretation. If a macroscopic time-dependent vector $f(t)$ (such as a malfunction) is formed as the superposition of numerous microscopic time-varying events $g_i(t)$ chosen from a set Γ, then the set of all such functions $f(t)$ will tend to be convex, regardless of the structure of the set Γ.

Acknowledgement

The author is indebted to Ms. Osnat Katzanek and to Mr. Dror Saddan for invaluable assistance in performing the computer calculations. This research was sponsored by the Air Force Office of Scientific Research, Air Force Systems Command, USAF, under grant number AFOSR-88-0209.

References

[1] Artstein, Z., On the Calculus of Closed Set-Valued Functions, Indiana University Math. J., 24: 433-41 (1974).

[2] Artstein, Z. and Hansen, J.C., Convexification in Limit Laws of Random Sets in Banach Spaces, Ann. Probab., 13: 307-9 (1985).

[3] Aumann, R.J., Integrals of Set-Valued Functions, J. of Math. Analysis and Applications, 12: 1-12 (1965).

[4] Baruh, H., Actuator Failure Detection in the Control of Distributed Systems, J. Guid. Cont. Dyn., 9: 181-9 (1986).

[5] Baruh, H., Sensor Failure Detection Method for Flexible Structures, J. Guid. Cont. Dyn., 10: 474-82 (1987).

[6] Bellman, R., *Introduction to Matrix Analysis*, 2nd Ed., Tata McGraw-Hill, 1974, p. 173.

[7] Ben Haim, Y., *The Assay of Spatially Random Material,* Kluwer Academic Publishers, Dordrecht, The Netherlands, 1985.

[8] Ben Haim, Y., Convexity analysis: A tool for optimization of malfunction isolation, 25th IEEE Conf. on Decision and Control, Athens, Greece, pp1570-5, 1986.

[9] Ben Haim, Y., Benchmarking the diagnosis of control actuator failures in linear systems, IFAC Conference on Advanced Information Processing in Automatic Control, 3-5 July (1989a), Nancy, France.

[10] Ben Haim, Y., Optimizing multi-hypothesis diagnosis of control-actuator failures in linear systems, AIAA Journal of Guidance, Control and Dynamics, to *appear* (1989b).

[11] Ben Haim, Y. and Elias, E., Indirect measurement of surface temperature and heat flux: Optimal design using convexity analysis, *Int'l. J. Heat Mass Transfer,* 30: 1673-83 (1987).

[12] Ben Haim, Y., and Elishakoff, I., Non-Probabilistic models of uncertainty in the non-linear buckling of shells with general imperfections: Theoretical estimates of the knockdown factor. ASME Journal of Applied Mechanics, to appear (1989).

[13] Bertsekas, D.P. and Rhodes, I.B., Recursive state estimation for a set membership description of uncertainty, *IEEE Trans.*, AC-16: 117-28 (1971).

[14] Bryson, A.E., Jr. and Ho, Y.C., *Applied Optimal Control*, John Wiley, New York, 1975, pp. 148-53.

[15] Caglayan, A.K., Necessary and Sufficient Conditions for Detectability of Jumps in Linear Systems, IEEE Trans., AC-25: 833-4 (1980).

[16] Fiorina M. and Maffezzoni, C., A Direct Approach to Jump Detection in Linear Time-Invariant Systems ···, IEEE Trans., AC-24: 428-34 (1979).

[17] Hardy, G.H., Littlewood, J.E. and Pólya, *Inequalities*, Cambridge University Press, (1934).

[18] Kerr, T.H., False Alarm and Correct Detection Probabilities Over a Time Interval for Restricted Classes of Failure Detection Algorithms, IEEE Trans., IT-28: 619-31 (1982).

[19] Massoumnia, M.A. and Vander Velde, Generating parity relations for detecting and identifying control system component failures, J. Guid. Cont. Dyn., 11: 60-65 (1988).

[20] Nash, R.A., Jr., Kasper, J.F., Jr., Crawford, B.S. and Levine, S.A., Application of Optimal Smoothing to the Testing and Evaluation of Inertial Navigation Systems and Components, IEEE Trans., AC-16:806-16 (1971).

[21] Rockafellar, R.T., *Convex Analysis*, Princeton University Pr., Princeton, 1970.

[22] Schmitendorf, W.E., Design methodology for robust stabilizing controllers, AIAA Journal of Guidance, Control and Dynamics, 10: 250-254, (1987).

[23] Schneider, D.L., *QFT Digital Flight Control Design As Applied to the AFTI/F16*, M.Sc. Thesis, Air Force Institute of Technology, Dec. 1986. Wright-Patterson Air Force Base, AFIT/GE/ENG/86D-4.

[24] Schweppe, F.C., Recursive state estimation: Unknown but bounded errors and system inputs, *IEEE Trans.* AC-13: 22-8 (1968).

[25] Schweppe, F.C., *Uncertain Dynamic Systems,* Prentice-Hall, Englewood Cliffs, N.J., 1973.

[26] Tempo, R., Robust estimation and filtering in the presence of bounded noise, IEEE Trans. on Automatic Control, 33: 864-867 (1988).

[27] Willsky, A.S. and Jones, H.L., A Generalized Likelihood Ratio Approach to the Detection and Estimation of Jumps in Linear systems, IEEE Trans., AC-21: 108-112 (1976).

[28] Witsenhausen, H.S., A minimax control problem for sampled linear systems, *IEEE Trans.*, AC-13: 5-21 (1968a).

[29] Witsenhausen, H.S., Sets of possible states of linear systems given perturbed observations, *IEEE Trans.*, AC-13: 556-8, (1968b).